# NAVAL POSTGRADUATE SCHOOL

**MONTEREY, CALIFORNIA**

# THESIS

**SOLUTION ANALYSIS OF UNIVERSAL WIRELESS JOINT POINT TECHNOLOGIES FOR HETEROGENEOUS TACTICAL NETWORKS**

by

Donald F. Stewart
Eric G. Turner

March 2006

| | |
|---|---|
| Thesis Advisor: | Alexander Bordetsky |
| Second Reader: | Eugene Bourakov |

**Approved for public release; distribution is unlimited**

THIS PAGE INTENTIONALLY LEFT BLANK

| | |
|---|---|
| **REPORT DOCUMENTATION PAGE** | *Form Approved OMB No. 0704-0188* |

| | | |
|---|---|---|
| **1. AGENCY USE ONLY *(Leave blank)*** | **2. REPORT DATE**<br>March 2006 | **3. REPORT TYPE AND DATES COVERED**<br>Master's Thesis |

| | |
|---|---|
| **4. TITLE AND SUBTITLE**: Solution Analysis of Universal Wireless Joint Point Technologies in Heterogeneous Tactical Networks | **5. FUNDING NUMBERS** |
| **6. AUTHOR(S)** Donald F. Stewart and Eric G. Turner | |
| **7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)**<br>Naval Postgraduate School<br>Monterey, CA 93943-5000 | **8. PERFORMING ORGANIZATION REPORT NUMBER** |
| **9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES)**<br>N/A | **10. SPONSORING/MONITORING AGENCY REPORT NUMBER** |

**11. SUPPLEMENTARY NOTES:** The views expressed in this thesis are those of the authors and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

| | |
|---|---|
| **12a. DISTRIBUTION / AVAILABILITY STATEMENT**<br>Approved for public release; distribution is unlimited | **12b. DISTRIBUTION CODE** |

**13. ABSTRACT (maximum 200 words)**

The scope of this thesis is to analyze the feasibility of having different wireless mesh network architectures transfer data to a wired network via a joint (universal) access point (UAP). Additionally this thesis analyzes the feasibility of using similar joint (universal) access point technology to allow heterogeneous wireless mesh network devices in close proximally to the UAP transmit data to/from each other via the UAP. This research also includes evaluating COTS tools for possible implementation of a joint access point as well as seeking partnership with private industry to assist in research efforts and/or the development or joint (universal) access point solution(s). The thesis concludes with a recommendation on application of universal joint point technology, to include recommendations for implementation of such technology in the Tactical Network Topology (TNT) environment.

| | |
|---|---|
| **14. SUBJECT TERMS**<br>AP/WAP, Interoperability, Heterogeneous Wireless Networks, UAP/UWAP | **15. NUMBER OF PAGES**<br>87 |
| | **16. PRICE CODE** |

| | | | |
|---|---|---|---|
| **17. SECURITY CLASSIFICATION OF REPORT**<br>Unclassified | **18. SECURITY CLASSIFICATION OF THIS PAGE**<br>Unclassified | **19. SECURITY CLASSIFICATION OF ABSTRACT**<br>Unclassified | **20. LIMITATION OF ABSTRACT**<br>UL |

THIS PAGE INTENTIONALLY LEFT BLANK

# SOLUTION ANALYSIS OF UNIVERSAL WIRELESS JOINT POINT TECHNOLOGIES IN HETEROGENEOUS TACTICAL NETWORKS

Donald F. Stewart
Lieutenant Colonel, United States Army
B.S., University of Southern Mississippi, 1986

Eric G. Turner
Lieutenant, United States Navy
B.S., Norfolk State University, 2000

Submitted in partial fulfillment of the
requirements for the degree of

**MASTER OF SCIENCE IN INFORMATION TECHNOLOGY MANAGEMENT**

from the

**NAVAL POSTGRADUATE SCHOOL**
**March 2006**

| | |
|---|---|
| Authors: | Donald F. Stewart |
| | Eric G. Turner |
| Approved by: | Alexander Bordetsky<br>Thesis Advisor |
| | Eugene Bourakov<br>Second Reader |
| | Dan C. Boger<br>Chairman, Department of Information Sciences |

THIS PAGE INTENTIONALLY LEFT BLANK

# ABSTRACT

Since its introduction in 1999, IEEE 802.11 standard has become the de-facto standard for wireless computing, but with the desire for increase range and mobility the standard is aggressively being challenged by new and emerging technology. Research conducted through ongoing Tactical Network Topology (TNT) experiments has successfully tested different types of wireless network technologies to include ITT MEA (MeshNetworks Enabled Architecture), Redline 802.16, and Flarion 802.20 in a mobile field environment. In each case, only the respective wireless access point technology (i.e., WAP with compatible 802.11, 802.16, 802.20 and ITT wireless interface card) could be used to transmit data into and across the TNT network and back to the LRV, TOC, and/or NOC at a given time. With different wireless technologies having their own advantages and disadvantages, the need for them to transfer data back and forth between wireless networks of different (i.e., heterogeneous) technologies and into a wired network, utilizing a common access point, is becoming increasingly important to wireless mobile devices users. Adding to this need is the desire to minimize equipment and personnel needed to support tactical, wireless network operations.

Sponsored by SOCOM and DoD, this thesis analyzes the feasibility of achieving interoperability between heterogeneous wireless networks via a joint (universal) wireless access point (UWAP/UAP). It studies the problems associated with why wireless devices built on different wireless technology are not interoperable with each other. It also details the requirements necessary to enable a single wireless access point to achieve universal interoperability with different wireless devices. Additionally, several COTS devices are evaluate for possible implementation of a universal wireless access point. The thesis concludes with recommendations on the application of universal, joint point technology, to include recommendations for implementation of such technology.

THIS PAGE INTENTIONALLY LEFT BLANK

# TABLE OF CONTENTS

# LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

# LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

# ACRONYMS AND ABBREVIATIONS

| | |
|---|---|
| 2.5G | Second and a Half Generation |
| 3G | Third Generation |
| 4G | Fourth Generation |
| AAA | Authentication, Authorization, and Accounting |
| AIM | Advanced Integration Modules |
| AODV | Ad-hoc On-demand Distance Vector |
| AP | Access Point |
| BS | Base Station |
| BSA | Basic Service Area |
| BSC | Base Station Controller |
| BSS | Base Service Set |
| BSSID | Base Service Set Identifier |
| BST | Base Station Transceiver |
| CAPWAP | Control and Provisioning of Wireless Access Point |
| CDMA | Code-Division Multiple Access |
| CF | Compact Flash |
| CME | Call Manager Express |
| COTS | Commercial Off-The-Shelf |
| CPT | CAPWAP Tunneling Protocol |
| CR | Camp Roberts |
| CWNP | Certified Wireless Network Professionals |
| DS | Distribution System |
| DSL | Digital Subscriber Line |
| DSR | Dynamic Source Routing |
| DSSS | Direct Sequence Spread Spectrum |
| EDGE | Enhanced Data GSM Environment |
| EMS | Element Management System |
| FCC | Federal Communications Commission |
| FDD | Frequency Division Duplexing |
| FHSS | Frequency Hopping Spread Spectrum |
| FLASH | Fast Low-Latency Access and Seamless Handoff |
| GLL | Generic Link Layer |
| GOTS | Government Off-The-Shelf |
| GPRS | General Packet Radio Service |
| GSM | Global System for Mobile-communication |

| | |
|---|---|
| HWIC | High-Speed WAN Interface Card |
| HP | Hewlett-Packard |
| HSDPA | High Speed Downlink Packet Access |
| HW | Hardware |
| IEEE | Institute of Electrical and Electronics Engineers |
| IOS | Internet over Satellite |
| ITT MEA | ITT MeshNetworks Enabled Architecture |
| JTRS | Joint Tactical Radio System |
| L2 | Layer 2 |
| L3 | Layer 3 |
| LAN | Local Area Network |
| LRV | Lightweight Reconnaissance Vehicle |
| LWAPP | Light Weight Access Point Protocol |
| MAC | Medium Access Control |
| MANET | Mobile Ad-hoc Network |
| MAV | Manned Aerial Vehicle |
| MBR | Mobile Broadband Router |
| NAC | Network Admission Control |
| NIC | Network Interface Card |
| NM | Network Modules |
| NOC | Network Operation Centers |
| OFDM | Orthogonal Frequency Division Multiplexing |
| OLSR | Optimized Link State Routing |
| oMG | Onboard Mobile Gateway |
| OSI | Open System Interconnection |
| PCMCIA | Personal Computer Memory Card International Association |
| PDA | Personal Digital Assistant |
| PDCP | Packet Data Convergence Protocol |
| PoE | Power Over Ethernet |
| QDMA | Quadrature Division Multiple Access |
| QoS | Quality of Service |
| RF | Radio Frequency |
| RIP | Routing Information Protocol |
| RLC | Radio Link Control |
| RR | Radio Router |

| | |
|---|---|
| SCA | Software Communications Architecture |
| SDR | Software Defined Radio |
| SOF | Special Operations Forces |
| SSCS | Service Specific Convergence Sub-Layer |
| SSID | Service Set Identifier |
| SW | Software |
| TAG | Technical Advisory Group |
| TNT | Tactical Network Topology |
| TOC | Tactical Operation Center |
| UAV | Unmanned Aerial Vehicle |
| UMTS | Universal Mobile Telecommunications System |
| UAP | Universal Access Point |
| UPnP | Universal Plug and Play |
| UPS | Uninterruptible Power Supply |
| UWAP | Universal Wireless Access Point |
| UWB | Ultra Wide Band |
| VIC | Voice Interface Cards |
| VPN | Virtual Private Network |
| VWIC | Voice/WAN Interface Card |
| WAP | Wireless Access Point |
| WIC | WAN Interface Card |
| WG | Working Group |
| WiDEN | Wideband Integrated Dispatch Enhanced Network |
| WNW | Wideband Networking Waveform |

THIS PAGE INTENTIONALLY LEFT BLANK

# ACKNOWLEDGMENTS

First and foremost, we would like to express our deepest gratitude to our Lord and Savior Jesus Christ for blessing us with not only the opportunity to fulfill a life-long aspiration of earning a Master's Degree but also for guiding us every day of our lives both in and out of the uniform. Secondly, we want to say "thank you" to the crown jewels of our lives, our lovely wives Drusilla Stewart and Charlene Turner for being a constant source of inspiration and encouragement throughout our military careers and especially while station here at Naval Postgraduate School. Their support and understanding during our course of studies and throughout the thesis process allowed us to dedicate valuable time that resulted in our ultimate success – your labors of love has not gone unnoticed, and we are forever grateful. Thirdly, we want to acknowledge our children for willingly sacrificing quality time with their fathers, which permitted us to excel in our profession. Next, we would like to thank Professor Alex Bordetsky for sharing with us his vision of a "Joint Point" concept and giving us the tools needed to make ground breaking advancements towards its development. Alone with Professor Bordetsky, we must thank Eugene Bourakov and Mike Clement for providing technical guidance during this process. Lastly, we would like to give thanks to our fellow NPS students, faculty, and industry partners, who provided critical data at certain junctions of this amazing race called the Master's Thesis process.

THIS PAGE INTENTIONALLY LEFT BLANK

# I. INTRODUCTION

## A. WIRELESS NETWORK ARCHITECTURES

In recent years, there has been extensive research on the validity of having a wireless network compliment or function in place of the traditional wired network. The advantages in this architectural shift are easily seen in both the commercial and military sectors. For instance, the cost alone, discounting timeliness and feasibility, in installing a wired network in large warehouses where point of sale electronic equipment is being used, in support of rescue/emergency operations, or in mobile military environments where communication suites are frequently being assembled and disassembled would make the use of wired network an impractical solution.

With the emergence of the wireless networking concept and the uncompromising need to communicate quickly, efficiently and effectively with collaborating agencies, people and devices, wireless technology has established a permanent foothold in the way communications are designed and implemented. However, to exploit the world of wireless networking better, a thorough understanding of the baseline architectures must be recognized. There are two prominent wireless network configurations, independent and infrastructure.[1]

First independent, this configuration can be broken down into two subcategories: ad-hoc (also known as peer-to-peer) and mobile ad-hoc network (MANET). Ad-hoc or peer-to-peer networks are typically used as a means of file sharing. These types of networks are defined as two or more computing devices (nodes), within equipment specific transmission/reception range, configured to exchange data (packets) directly between nodes as depicted in Figure 1. The limited amount of time it takes for configuration and setup are one of the many advantages of communicating via an ad-hoc configuration.

[1] Planet3 Wireless, CWNA Certified Wireless Network Administrator Official Study Guide (Exam PWO-100) 3rd Edition, (McGraw-Hill and Osborne, 2005), 329-331.

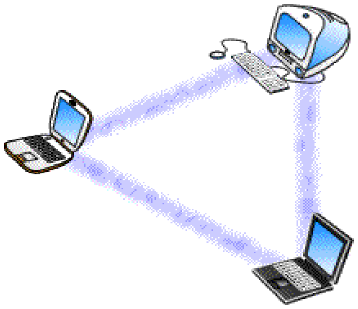


Figure 1. Ad-hoc (peer-to-peer) Network[2]

MANET technology is analogous to Mobile Packet Radio Networking, Mobile Mesh Networking, and Mobile Multi-hop Wireless Networking[3]. In efforts to minimize confusion as to which mobile-like technology we are referring to, we will henceforth categorize them under one umbrella – wireless mesh networks. Wireless mesh networks function similar to that of ad-hoc networks in that it not only exchanges data directly between nodes but it can also use any given node as a conduit to transmit packets to other nodes that are outside its transmission/reception range but within the transmission/reception range of another node. In addition, mesh protocols possesses the decision-making ability to add and remove nodes with similar capabilities to and from their existing wireless network. The signal strength between nodes is the key factor in this process (see Figure 2 below). In other words, mesh architectures are self-forming and self-healing networks making it extremely dynamic and flexible, which is ideal for highly versatile mobile environments.

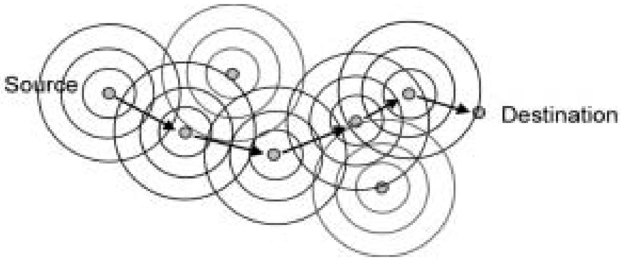


Figure 2. Wireless Mess Network[4]

[2] From: VICOMSOFT Corporation, *Support–White Papers–Wireless Networking*. http://www.vicomsoft.com/knowledge/reference/wireless1.html#1, Last Accessed 05 Oct 05.

[3] S. Corson and others, *Mobile Ad hoc Networking (MANET). RFC 2501*, Internet Engineering Task Force (IETF), Jan 1999, 2.

[4] From: Source unavailable as of Mar 06.

The second wireless configuration is an infrastructure network. This type of configuration utilizes a wireless access point (WAP) device and is primarily designed to connect a wireless network to a wired network as illustrated in Figure 3. An important detail to note concerning an infrastructure network is that although an infrastructure network normally has wireless nodes associated with it, this is not a requirement for it to carry that classification. The infrastructure network will be discussed in more detail in subsequent paragraphs.

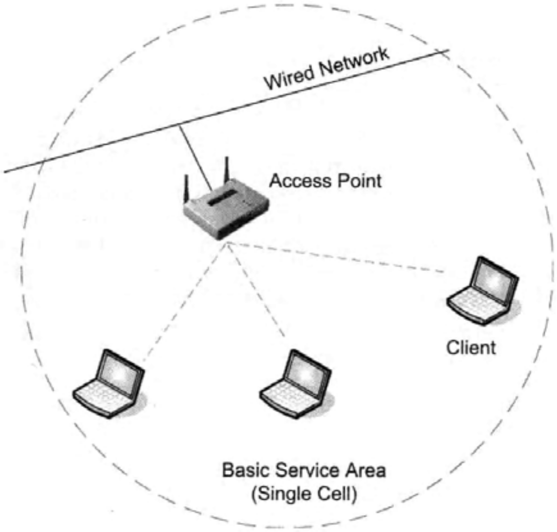


Figure 3. Infrastructure Network[5]

## B. WIRELESS COMMUNICATIONS IN CURRENT TACTICAL NETWORK TOPOLOGY (TNT) OPERATIONS

The Tactical Network Topology (TNT) experiments are a string of experiments designed to explore the technologies of mobile and Manned/Unmanned Aerial Vehicle (MAV/UAV) networks in support of Special Operations Forces (SOF) in combat using various wireless communications and sensors. Supported by a collaborative effort between NPS departments, military units, and civilian contractors these experiments support the enhancement of the SOF war fighting capabilities. One of the major focuses of TNT is on the self-forming, self-healing multi-path wireless network that exhibits characteristics of both the mesh network and the infrastructure network.

[5] From: Planet 3 Wireless, 221.

### 1. Mesh Network (MN) within TNT

The mesh network consisted of tacticomps (a.k.a. rugged PDAs (Personal Digital Assistants)), tactical balloons, MAV/UAVs, and laptops mounted in Lightweight Reconnaissance Vehicles (LRVs) configured for a mesh-networking environment. The idea behind mesh technology is that each node in the network can serve as an access point with routing capabilities, so communication can be routed through any accessible or nearby node to reach back to the TOC (located at Camp Roberts (CR)). (See Figure 4)

### 2. Infrastructure Network within TNT

In simplest terms, the TNT infrastructure network (particularly at CR TOC) consists of a wired network that extends network services to both wired and wireless host. The key and unique factor surrounding this configuration is the variety of associated WAPs. As illustrated in Figure 1-4, this network has the ability to connect to, receive, and forward 802.3 packets to 802.11, 802.16, 802.20, or ITT MEA (MeshNetworks Enabled Architecture) wireless nodes. Communication to and from the 802.3 Ethernet is facilitated through these various AP devices to include 802.11b/g WAPs, 802.16 AN-50e terminals, ITT Intelligent WAPs, and 802.20 base stations.

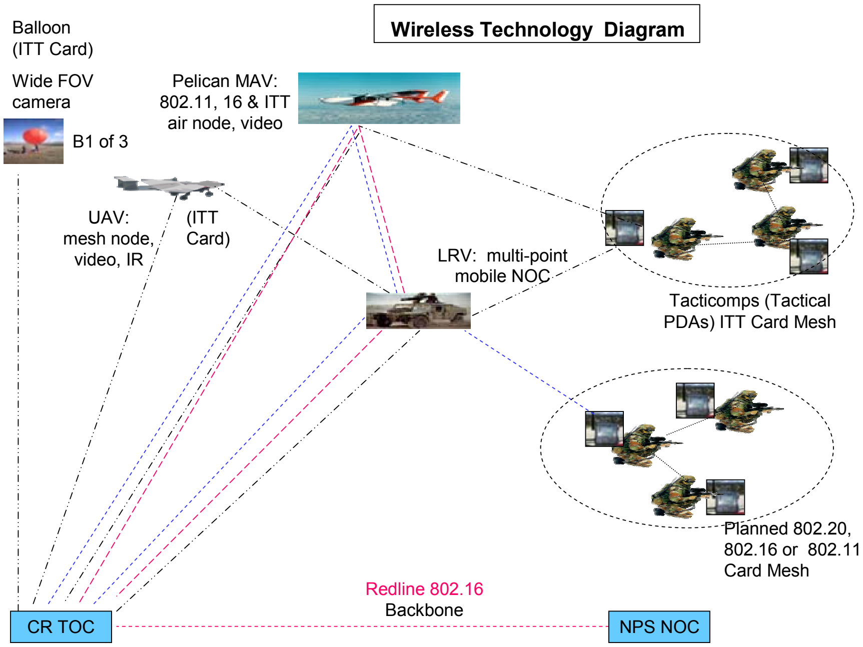


Figure 4. TNT Wireless Mesh Network Layout

The experiments analyzed and documented in this thesis falls under the infrastructure network configuration. Several routing algorithms and protocols are used to provide the functionality for the wireless portion of this infrastructure network.

## C. WIRELESS ACCESS POINT FUNCTIONALITY AND CHARACTERISTICS

A Wireless Access Point (WAP), often referred to as just Access Point (AP), is a hardware device (or software application residing on a computing device) that acts as a communication hub for users of a wireless device (client) to connect to a wired or wireless network. The WAP provides wireless communication devices a wireless point of access into a network. Figure 5 depicts hardware (HW) & software (SW) wireless access points.

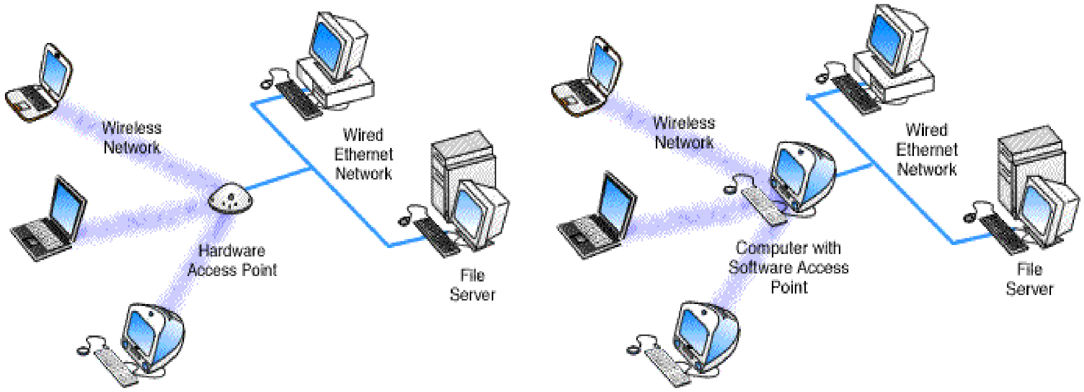


Figure 5. Hardware & Software Wireless Access Points[6]

Usually connected to a wired network, a WAP is generally used to relay data between two or more devices on the wireless network or to relay data between one or more devices on the wireless network to one or more devices on the wired network. In the later instance, the WAP acts as a gateway for wireless clients to access the wired network. Although a WAP usually connects wireless clients to a wired LAN, this does not always have to be the case. A WAP could be used to bridge two wired LANs, connecting wired clients of one LAN to wired clients of another LAN. WAPs are also important for extending the physical range of LAN services making them accessible to

[6] After: VICOMSOFT Corporation.

wireless users. Within the range of the WAP, the wireless end-user essentially has a full network connection with the added benefit of mobility. Although not practiced in the vast majority of currently installed IEEE 802.11 networks, a WAP may also act as the network's arbitrator, negotiating when each nearby client device can transmit.[7] Additionally, many WAPs can be connected together to create a larger network that facilitate "roaming". In this instance, a series of access points could be spread over a large area, connected to the same network (or to different networks), providing hotspots[8] where wireless clients can connect to the network without regard to any particular AP while moving from one spot to another (i.e., roaming). This concept is somewhat incidental in places where a combination of coffeehouses, cafes, and other public spaces offering wireless access allow anonymous clients to roam over a large area, staying more or less continuously connected.

To perform the functions described above the wireless AP operates in various modes. The CWNA Official Study Guide describes three modes in which a wireless access point can be configured to operate in. These modes include “root” mode, “repeater” mode, and “bridge” mode.[9] In root mode, the AP is connected to a distribution system through its Ethernet interface and serves as a gateway for wireless clients. Figure 6 depicts APs operating in root mode.

[7] Wikipedia, The Free Encyclopedia, http://en.wikipedia.org/wiki/Wireless_access_point, Last accessed 06 Oct 05.

[8] Hotspots are locations where you can have access from mobile computers (such as a laptop or a PDA) without connection cables to networked services such as the Internet. Hotspots are often found near restaurants, train stations, airports, cafes, libraries and other public places. Source: Wikipedia, The Free Encyclopedia, http://en.wikipedia.org/wiki/Hotspot_%28wifi%29, Last accessed 10 Dec 05.

[9] Planet 3 Wireless, 222-223.

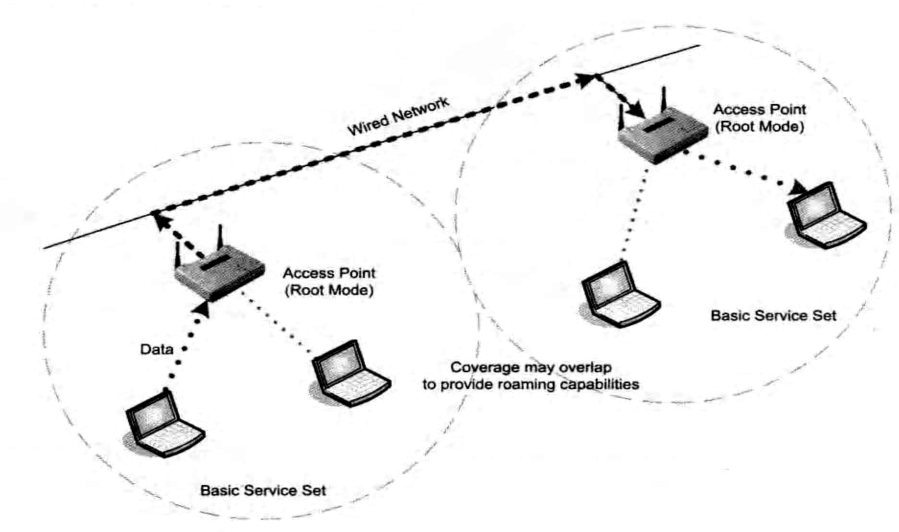


Figure 6. Two Access Points in Root Mode[10]

In repeater mode, the AP is connected to a root AP and provides intermediate connectivity between the root AP and wireless clients that are out of range of the root AP. The repeater AP acts as a wireless relay, extending the range of the root AP. Figure 7 depicts an access point operating in repeater mode.

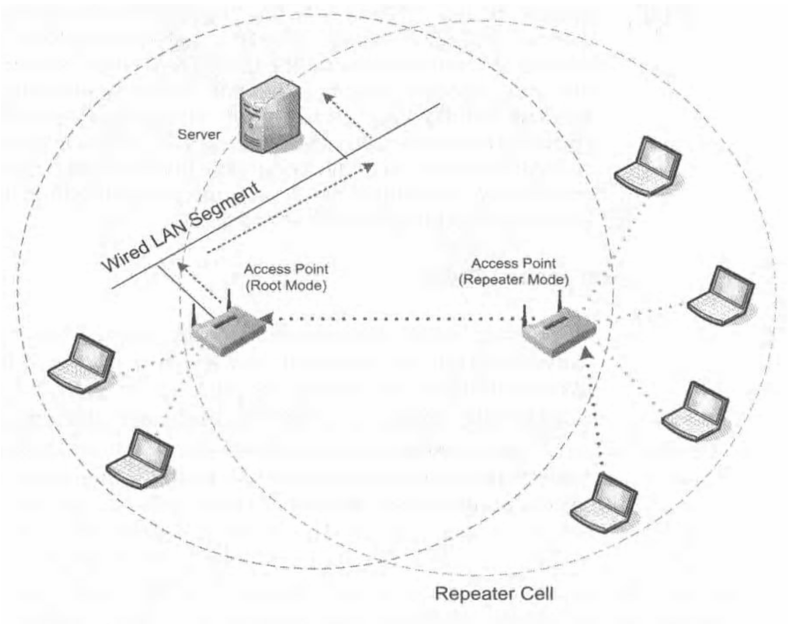


Figure 7. Access Point in Repeater Mode[11]

[10] From: Planet 3 Wireless, 223.

[11] Ibid, 226.

In bridge mode, APs are used to create a wireless link between two wired LAN segments. Access Points in bridge mode associate only with each other and typically do not allow associations from wireless clients. Figure 8 below displays two APs in bridge mode connecting two wired LAN segments.

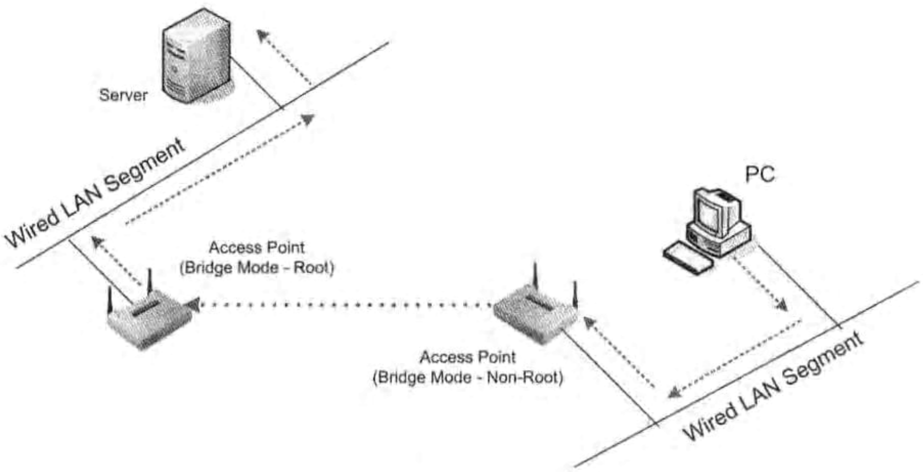


Figure 8. Access Points in Bridge Mode[12]

Wireless access points characteristics and capabilities vary with the make and model of each AP device. Such characteristics include transmission power, reception range, spectrum compatibility, maximum physical/data rate, and the maximum number of clients that can be serviced by the WAP. Today's IEEE 802.11 WAPs can typically communicate with up to 30 client systems within a radius of about 100 m.[13] However, communication ranges vary a lot depending on such variables as indoor or outdoor use, type of antenna, operating radio frequency, height above ground, nearby obstructions, operating weather conditions, and power output of the device. Transmission (output) power and antenna reception effect the size of the coverage area of the WAP. As the transmission power and the AP's reception range increases, the coverage area also increases allowing wireless clients to operate farther from the AP without loosing connectivity. Because properly adjusting the coverage area is so important to wireless network performance, many WAPs come with adjustable transmission power and detachable antennas that allow the user to attach a different set of antennas to the AP.

[12] From: Planet 3 Wireless, 224.

[13] Wikipedia, The Free Encyclopedia, http://en.wikipedia.org/wiki/Wireless_access_point, Last accessed 06 Oct 05.

The AP radio card(s), normally in the form of a PCMCIA card, is a huge determinant in the number of users, frequency spectrum compatibility, maximum physical/data rate, and other functionalities of the AP. Therefore, some access points have removable radio cards. This is generally accomplished by installing PCMCIA slots onto the AP.

## D. PROBLEM DEFINITION AND SCOPE OF THESIS

Research conducted through ongoing TNT experiments has successfully tested different types of wireless network technologies (i.e., 802.11, 802.16, 802.20 and ITT) in a mobile field environment. In each case, only the respective wireless access point technology (i.e., WAP with compatible 802.11, 802.16, 802.20 and ITT wireless interface card) could be used to transmit data into and across the TNT network and back to the LRV, TOC, and/or NOC at a given time. With wireless mesh technologies having their own advantages and disadvantages, the need for them to transfer data back and forth between wireless networks of different technologies and into a wired network, utilizing a common access point, is becoming increasingly critical for joint and coalition operations. Adding to this need is the desire to minimize equipment and personnel support needed to support tactical, wireless network operations.

Therefore, the scope of this thesis was to analyze the feasibility of having different wireless mesh network architectures to transfer data to a wired network or wireless long-haul backbone via a joint (universal) access point. Additionally, this thesis analyzed the feasibility of using similar joint (universal) access point technology to allow different wireless mesh network architectures in close proximity to transmit data to/from each network. This research also evaluated COTS tools for possible implementation of a joint access point as well as evaluated partnership with private industry to assist in research efforts in developing joint access point solution(s). The thesis concludes with a recommendation on application of universal, joint point technology, to include recommendations for implementation of such technology.

THIS PAGE INTENTIONALLY LEFT BLANK

# II. PROBLEM ANALYSIS

## A. LIMITATIONS IN CURRENT ACCESS POINT TECHNOLOGIES

With the proliferation of wireless computing and wireless networks, many vendors market wireless access points. Therefore there are many different commercial WAPs, some even integrated with a cable modem or DSL router and firewall. These special-purpose devices are convenient, but they tend to be inflexible, lacking interoperability with APs produced by other vendors and with wireless devices built on differing wireless technologies. Observation made during the study of WAPs used in TNT experiments included:

- APs built to support different wireless technologies could not wirelessly communicate with each other (e.g., 802.11 ITT AP built to support devices operating on 2.4 GHz could not communicate with 802.20 base station built to support devices operating on 3.5 GHz).
- APs of different vendors built to support the same wireless technology (802.11) could not communicate with each other (i.e., 802.11b/g WAP could not communicate with an 802.11 ITT Intelligent WAP).
- Wireless devices could only communicate with WAPs built on the same wireless technology (i.e., 802.11b/g devices could only communicate with a 802.11b/g WAP, ITT MEA wireless devices could only communicate with a ITT Intelligent WAP, and 802.20 devices could only communicate with a 802.20 base station)

These limitations found in WAPs utilized in TNT appeared to be the norm rather than the exception and were determined to be caused by a number of factors associated with wireless networks. These factors include relaxation of wireless standards, frequencies used by wireless devices, radio frequency (RF) spread spectrum and modulation techniques, and OSI (Open System Interconnection) layer 2 connectivity used in TNT wireless devices.

### 1. Shortcoming in Wireless Technology Specifications

To begin with, different standards bodies establish the standards for the 802 wireless technologies, mainly layer 1 and 2 of the OSI Reference Model. Although the IEEE 802 Project (or LAN/MAN Standards Committee) Sponsor Executive Committee and IEEE Standard Board preside as the over watching standards bodies for the 802 family of technologies, each of the 802 technologies (i.e., 802.11, 802.16, and 802.20) have their own Working or Technical Advisory Group (WG/TAG). Within each WG/TAG there are generally several working groups. These working groups evaluate proposals and drafts standards to address specific requirement(s) within a specific 802 technology. This has led to multiple and different standards amongst the various 802 wireless technologies making interoperability difficult.

Secondly, "many commentators have attributed interoperability problems to ambiguities in specification."[14] In general, a standard (specification) is designed to be flexible so that it is applicable to the greatest variety of implementations. In a highly competitive market, this can led to vendors implementing slightly differing solutions for the same wireless standard in an effort to optimize their design in unique ways and therefore add value to their product. Such differences in implementation may prevent different devices [of the same technology family] from communicating at all.[15] Additionally, although IEEE has published recommended practices, existing wireless standards do not specify the communications protocols required to support interoperability between access points from different vendors. This ambiguity or lack of specification in inter-access point communication further contributes to interoperability problems. In the case of the WAPs deployed in previous TNT experiments, these specification shortcomings contributed to the inability of WAPs of different wireless technologies from being able to communicate wireless with each other.

### 2. Frequencies & Spread Spectrum Technologies

The 802.11b/g wireless access points used within TNT were Linksys WAP54G 802.11b/g WAPs. These WAPs operate in the unlicensed 2.4 GHz frequency band (2.40 - 2.4835 GHz range). They received and transmitted signal transmissions using both

[14] Dr. Sadie Creese and others, *Interoperability Challenges for Wireless Communication*, QinetiQ, 31 March 2003, 9. http://www.nextwave.org.uk/downloads/forward_icwc.pdf, Last accessed 09 Dec 05.

[15] Ibid, 10-18.

Direct Sequence Spread Spectrum (DSSS)[16] and Orthogonal Frequency Division Multiplexing (OFDM)[17] modulation technique.[18] Equipped with 802.11b/g PCMCIA client cards, these WAPs were only able to communicate wirelessly with 802.11b and 802.11g devices and were not able to communicate with 802.11 ITT devices or 802.11 ITT WAPs. Nor were they able to communicate wirelessly with 802.16 or 802.20 devices or their respective access points. Figure 9 depicts a Linksys WAP54G 802.11b/g.

Figure 9. Linksys WAP54G 802.11b/g WAP[19]

The ITT Intelligent WAP (IAP 6300), pictured below in Figure 10, was equipped with a WMC6300 PCMCIA wireless client card and also operate in the unlicensed 2.4 GHz frequency band (advertised as 2.40 - 2.4835 GHz range). However, instead of using DSSS or OFDM signal spread spectrum technology and modulation techniques, this WAP used proprietary transmission and processing methods to receive and transmit RF signals. This proprietary technology is referred to as Quadrature Division Multiple Access (QDMA) and the specifics surrounding this modulation technique is not fully

[16] DSSS is a transmission technology used to increases a signal's resistance to interference. DSSS works by combining the data signal at the sending station with a higher data rate bit sequence or chipping code (a pseudorandom number (PN) sequence of 1 and −1 values), that divides the user data according to a spreading ratio. The chipping code is a redundant bit pattern for each bit that is transmitted, which increases the signal's resistance to interference. If one or more bits in the pattern are damaged during transmission, the original data can be recovered due to the redundancy of the transmission. http://www.webopedia.com/TERM/D/DSSS.html, Last accessed 08 Nov 05.

[17] OFDM is a frequency division multiplexing modulation technique for transmitting large amounts of digital data over a radio wave. OFDM works by splitting the radio signal into multiple smaller sub-signals that are then transmitted simultaneously at different frequencies to the receiver. OFDM reduces the amount of crosstalk in signal transmissions. 802.11a, 802.11g, and 802.16 technologies use OFDM. http://www.webopedia.com/TERM/O/OFDM.html, Last accessed 08 Nov 05.

[18] Linksys Wireless-G WAP54G 802.11b/g Wireless Access Point: Product Features, http://www.dealtime.com/xPF-Linksys_Wireless_G_Access_Point_WAP54G, Last accessed 10 Dec 05.

[19] Ibid.

known.[20] We concluded that this proprietary frequency modulation technique added to the limitation of this AP inability to communicate wirelessly with other devices not equipped with the Motorola WMC6300 PCMCIA.

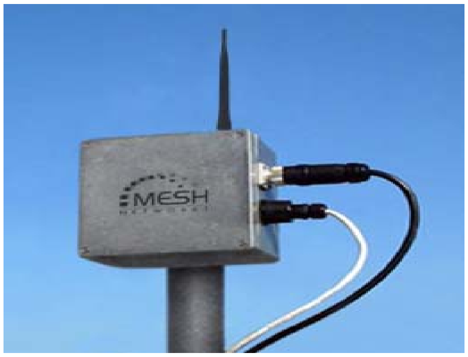


Figure 10. ITT Intelligent AP[21]

Although the 802.16 AN-50e terminals deployed in TNT experiments utilize OFDM technology, they were not able to communicate wirelessly with 802.11 devices or WAPs that also utilized OFDM spread spectrum technology. These wireless access terminals, produced by Redline Communications, operate in the unlicensed 5.4 and 5.8 GHz frequency bands vices the 2.4 GHz band used by the 802.11 devices.[22] A Redline AN-50e Terminal along with associated flat panel antenna and mounting bracket is pictured in Figure 11 below.

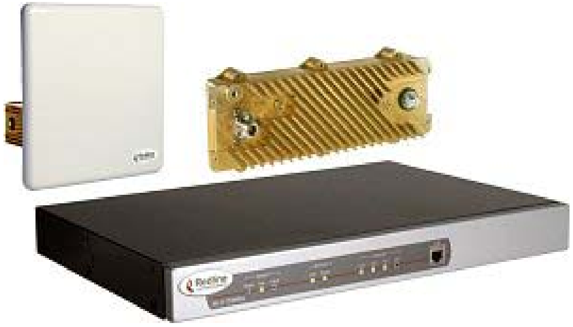


Figure 11. Redline 802.16 AN-50e Terminal[23]

[20] Eric Smith, *MeshNetworks Gets FCC Approval*, 13 Nov 02, http://www.wi-fiplanet.com/news/ article.php/1500101, Last accessed 23 Jan 06.

[21] From: Mesh Networks, IAP6300 Intelligent Access Point Brochure, MeshNetworks, Inc, 2002, http://www.cwti.us/brochure/CWTI-Technology_Mesh-IAP6300.pdf, Last access 10 Dec 05.

[22] Redline Communications, *Datasheet: AN-50e Wireless Broadband*, Redline Communications Inc., http://www.redlinecommunications.com/products/an50/AN-50.pdf, Last accessed 10 Dec 05.

[23] Ibid.

The 802.20 RadioRouter Base Station (BS) used in TNT 05-4 was provided by Flarion Technologies and is both a wireless base station and an IP access router.[24] Depicted in Figure 12 below, this base station operates on the licensed only frequencies that range between 400 MHz and 3.5 GHz and built is on Flarion's FLASH-OFDM (Fast Low-Latency Access and Seamless Handoff - Orthogonal Frequency Division Multiplexing) technology for reception and transmission of RF signals.[25] Utilizing this proprietary modulation technique, which specifies higher layer protocols than the normal OFDM, and operating only on licensed frequencies, the Flarion 802.20 RadioRouter BS communicated wirelessly only with devices equipped with the Flarion FPC 2500 Wireless Network Cards.[26]

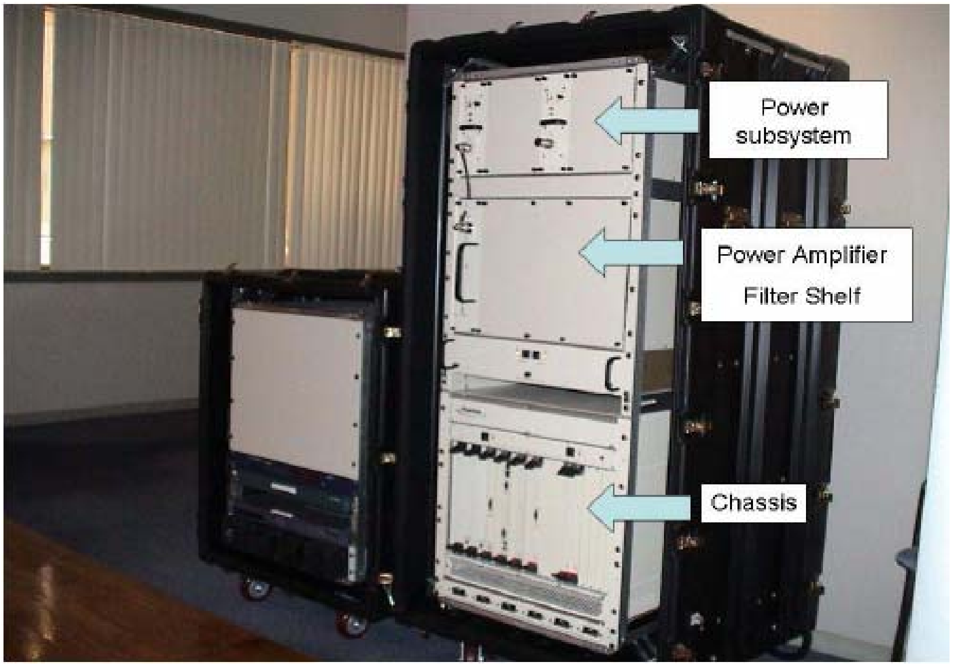


Figure 12. 802.20 Indoor RadioRouter Base Station[27]

[24] William J. Parish and Daniel R Tovar, *Tactical Wireless Networking in Coalition Environments: Implementing an IEEE 802.20 Wireless End-User Network Utilizing Flash-OFDM to Provide a Secure Mobile Extension to Existing WAN*, Master's Thesis, Naval Postgraduate School, Monterey, California, Sept 2005, 24.

[25] Flarion, Product and Technology: *RadioRouter Base Station*, Flarion Technologies Inc., 2003-2005, http://www.flarion.com/products/radio_router.asp, Last accessed 10 Dec 05.

[26] Flarion, Product and Technology: *Wireless Network Cards*, Flarion Technologies Inc., 2003-2005, http://www.flarion.com/products/cards.asp, Last accessed 10 Dec 05.

[27] From: Parish and Tovar, 25.

### 3. Layer 2 Connectivity

An additional factor to consider surrounding the limitations found in infrastructured networks is which layer of the OSI Reference Model (layer 2 – data link or layer 3 – network) the given WAP or base station device is operating within. Considering that one of the main functions of an AP is to route data grams from a wireless network to the wire network and vice versa, and considering that routing is a function normally conducted at layer 3, routing devices and their associated routing protocols are typically network-layer entities. However, an AP is a layer 2 device and it is at this layer it receives data transmissions from any number of wireless nodes.

Layer 2, the data link layer, is regarded as one of the most important layers in the OSI model. At this layer, error control, flow control, addressing, framing, medium access control, and similar functions are performed. It is also at this layer where two wireless communicating devices (e.g., wireless node and WAP) initiate and negotiate a communication connection. To accentuate the impact layer 2 has on wireless interoperability: (1) provided below is a general explanation, based on the 802.11 standards, of how the layer 2 connectivity process works, and (2) ensuing this explanation are specific layer 2 descriptions of most of the wireless technologies used within TNT experiments.

For a wireless device (node) to join a network via a WAP, two processes called authentication and association has to be performed successfully. However, before this can occur, a node has to first discover a BSS (Basic Service Set) to join. In an infrastructured network, a BSS is identified by a fixed 48-bit hexadecimal value known as BSS Identifier (BSSID). Basic Service Sets (BSS's) consists of nodes that are within a designated proximity of each other. However, being in close proximity to other nodes or a WAP does not guarantee a node inclusion in a given BSS. In other words, a node has to request to be a part of a BSS, which is performed by interacting with an access point. This process is initiated when a node scans and locates a BSS or when a WAP begins radiating. There are three frame types associated with this scanning process: beacons, probe requests, and probe responses. Beacons are used by the AP and they contain information such as time synchronization, SSID information, traffic indication map, supported rates of the network (i.e., speed in Mbps), and Frequency Hoping Spread

Spectrum (FHSS) or Direct Sequence Spread Spectrum (DSSS) parameter sets. Nodes utilizing active scanning will send out probe requests. These requests are sent out in search for a BSS with a particular SSID or the SSID value could have a null value assigned to it meaning the scan will look for any SSID. Once a BSS is discovered that meets the parameter configuration, the AP (or base station) will respond with a probe response.

The authentication process is the next process to transpire after the wireless node discovers the WAP. Authentication is simply verifying that a node has permission to communicate with a WAP. A node can only become associated with a WAP after it has authenticated with the WAP. There are two types of authentication: Open System Authentication and Shared Key Authentication. Once a node successfully authenticates with the WAP then the association process starts. This process is a request from a remote node to join (send data to) a given BSS (network) via a WAP. Similar to discovering an AP, the association phase also involves sending frames between the AP and the node. In this case, the node will send an association request frame to the AP and in turn, the AP will respond with an association response frame. This process will result with an acceptance or rejection to send data over the network by either forwarding or ignoring the data from the wireless node. In other words, if the wireless node fails to provide the appropriate authentication or the frames sent by the wireless node are unrecognizable by the WAP, the data from the wireless node will be ignored. Another restricting factor in this process is that a node can only be associated with one BSS at a time.[28]

### *a. Data Link Layer Purpose & Composition*

In 802.11x technologies, the Data Link Layer (i.e., layer 2) can be broken down into two sub-layers: Logical Layer Control that addresses the error and flow control; and the Medium Access Control that performs addressing, framing, and medium access control functions (see Figure 13).[29] As mentioned earlier in this thesis, recent TNT experiments also used a proprietary wireless technology called ITT MEA, which is a remote relative to the 802.11 family standards. Due to its proprietary nature, we were

[28] Planet 3 Wireless, 331-344.

[29] C. Siva R. Murthy and B. S. Manoj, Ad Hoc Wireless Networks: Architecture and Protocols, Prentice Hall PTR, 2004, 47.

unable to locate diagrams of its data link layer or data frame format. However, because of its close relations to 802.11 standards, we suspect its data link layer resembles that of the 802.11x technology.

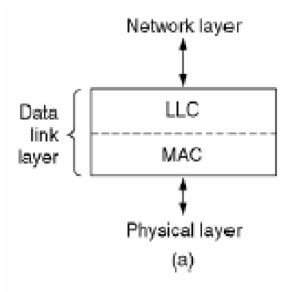


Figure 13. 802.11 Data Link Layer[30]

Continuing, for 802.16 technologies, the data link layer is sub-divided into three sub-layers: Service specific convergence sub-layer (SSCS), MAC sub-layer, and Security sub-layer (see Figure 14). The SSCS offers transformation and mapping of external network data support for both ATM and Packet based architectures. The MAC sub-layer contains the MAC rules and provides system access, bandwidth allocation and connection maintenance support. Lastly, the security sub-layer ensures user privacy by playing a key role in the authentication and secure key exchange process when applicable.[31]

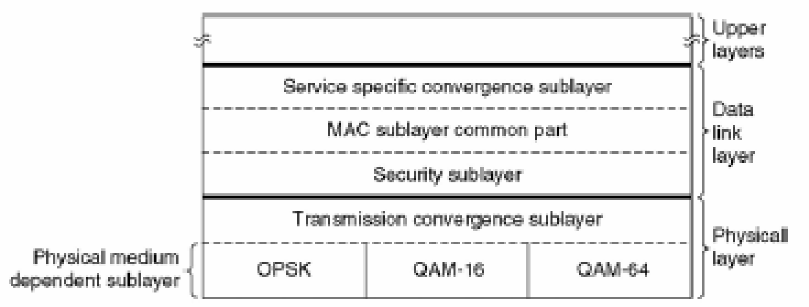

Upper layers
Service specific convergence sublayer
MAC sublayer common part
Security sublayer
Data link layer
Transmission convergence sublayer
Physicall layer
Physical medium dependent sublayer
OPSK
QAM-16
QAM-64

Figure 14. 802.16 Data Link Layer [32]

[30] From: Iowa State University – Department of Computer Science, http://www.cs.iastate.edu/~cs586/f04/notes/ chapter4_2.pdf, slide 29, Last accessed 20 Dec 05.

[31] T. Al Mosawi and others, *Centre for Telecommunications Research - Review of Existing Mobile Broadband Wireless Access (MBWA) Technologies (IEEE 802.16 and IEEE 802.20).* King's College London - University of London, Nov 2004, 17-18.

[32] From: Iowa State University, slide 40.

The 802.20's data link layer functionality is similar to that of 802.16 concerning its bridge/management data characteristics, but its configuration resembles 802.11's data link layer structure. The 802.20's MAC sub-layer is used to schedule resource assignments, perform efficient packet switching over the air, and provide hooks to handle QoS. Its logical link sub-layer uses local (as opposed to end-to-end) feedback to create a very reliable link from an unreliable wireless channel, with very low delays (see Figure 15).[33] Nonetheless, in spite of this somewhat detailed description of 802.20's data link layer, their standards are not as far along or as defined as 802.11 or 802.16 due to it being a recently embarked upon technology still under development.

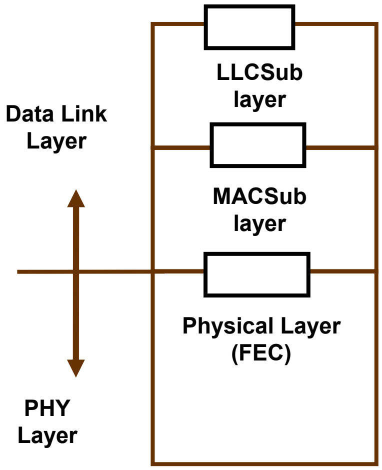


Figure 15. 802.20 Data Link Layer[34]

### *b. Data Frame Format*

As mentioned earlier, information is passed between APs and nodes at layer 2, which is performed through the uses of data frames. The format of these frames is technology specific meaning that the data link layer information, MAC header information in particular, varies between technologies. These variances, to which some

[33] Flarion Technologies, Inc., *Whitepaper – OFDM for Mobile Data Communications*. http://www.flarion.com/products/whitepapers/OFDM_Mobile_Data_Communications.pdf. Mar 2003, Last accessed 23 Dec 05.

[34] From: IEEE Standards Association, http://grouper.ieee.org/groups/802/20/WG_Docs/802.20-03-16r1.ppt, Last accessed 27 Dec 05.

are due to proprietary design, also decrease interoperability between different wireless technologies. Differences in these headers are depicted in Figures 16 through 18 below (ITT MEA data frame formats is not included due to accessibility).

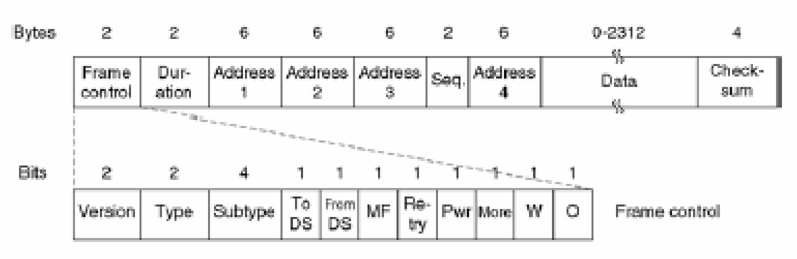


Figure 16. 802.11 Data Frame[35]

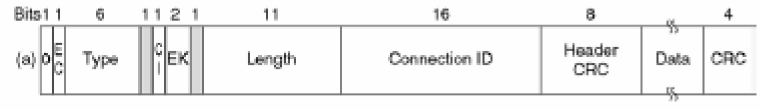


Figure 17. 802.16 Data Frame[36]

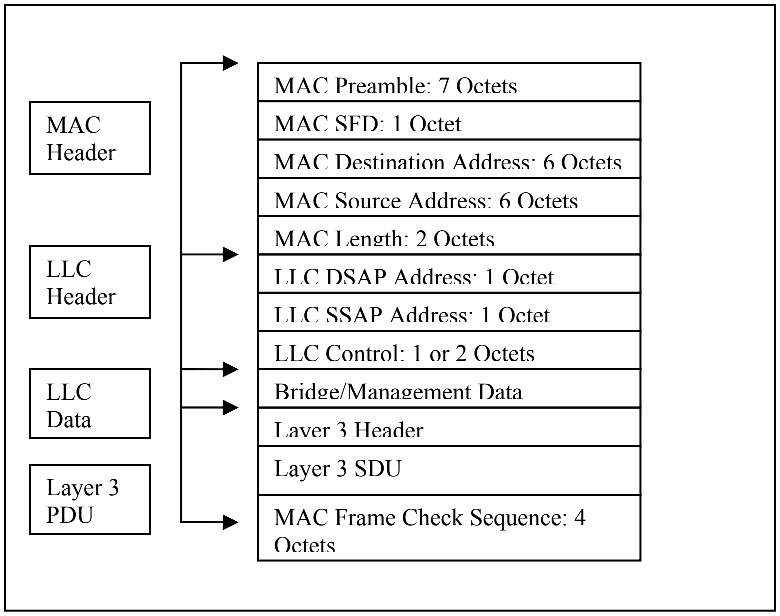

MAC Header
LLC Header
LLC Data
Layer 3 PDU
MAC Preamble: 7 Octets
MAC SFD: 1 Octet
MAC Destination Address: 6 Octets
MAC Source Address: 6 Octets
MAC Length: 2 Octets
LLC DSAP Address: 1 Octet
LLC SSAP Address: 1 Octet
LLC Control: 1 or 2 Octets
Bridge/Management Data
Layer 3 Header
Layer 3 SDU
MAC Frame Check Sequence: 4 Octets

Figure 18. 802.20 Data Frame [37]

[35] From: Iowa State University, slide 36.

[36] Ibid, slide 44.

[37] From: IEEE 802, LAN/MAN Standards Committee, http://www.ieee802.org/1/linksec/Docs/LAN_Threat_Assessment_Rev.1.doc, page 5, Last accessed 22 Dec 05.

## III. DEFINITIONS, REQUIREMENTS, & SPECIFICATIONS FOR A UNIVERSAL WIRELESS ACCESS POINT

A universal wireless access point (UWAP) is a device that would allow full interoperability among the most widely used wireless networking standards. The UWAP, or universal access point (UAP) for short, acts as both the wireless gateway to the LAN and a protocol translator between wireless devices of different wireless standards. To be effective in the TNT heterogeneous wireless mesh network environment, a UAP must be able to receive and transmit on the full range of radio bands associated with the wireless technologies utilized (i.e., 802.11, ITT, 802.16, and 802.20). Additionally, a UAP must be able to interpret various modulations and spread spectrum techniques. It should also have the capability to perform frequency adaptation, modulation and spread spectrum translation, and layer 2 protocol access control and translation. Furthermore, to facilitate QoS negotiation-renegotiation on behalf of the heterogeneous wireless devices, a UAP should possess the capacity to store network and devices information, capabilities, and preferences. Finally, the UAP should be able to perform handoffs as the mobile wireless devices roams (i.e., moves) from one UAP to another.[38] In addition to the components and capability that the traditional wireless access point possesses, to perform these functions listed above a UAP should be equipped with an intelligent antenna system and a layer 2 protocol bridging system. Moreover, to facilitate easy upgradeability the definitive UAP should be designed on the concept of a software defined radio system. For an intuitive analogy of how a universal wireless access point would function, consider the following scenario:

- Imagine a meeting in a conference room of five people that speak five different languages (i.e., different heterogeneous wireless devices). To facilitate this meeting a translator that is fluent in each of these five

[38] Upkar Varshney and Radhika Jain, *Issues in Emerging 4G Wireless Networks*, Georgia State University, http://www.ee.oulu.fi/~skidi/teaching/mobile_and_ubiquitous_multimedia_2002/ issues_in_emerging_4G_wireless_networks.pdf, Last accessed 05 Dec 05.

- languages (i.e., a UAP) is brought into the conference room and position so that he/she can hear and be heard by each of the five people. The five meeting attendees are informed that:

  (1) all communication must go through the translator,

  (2) only one person can talk at a time,

  (3) you must ensure no one else is talking before you speak or be granted permission to speak by the translator, and

  (4) before addressing another person, you must first identify the name(s) of the person(s) you want to address.

- When an attendee speaks, the translator (UAP) hears the speaker's voice (signal) through his/her two ears, the receiver part of the intelligent antenna system.
- The translator's brain, a specialized signal processor, determines what language the speaker is speaking, what language the intended addressee(s) speaks, and converts the message into the appropriate language for the addressee(s).
- Using his/her mouth, the transmitter part of the intelligent antenna system, the translator first informs all attendees to stand by and then communicates the translated message to the intended addressee(s).

Figure 19 below models the utilization of a universal wireless access point (UWAP/UAP) in the TNT network.

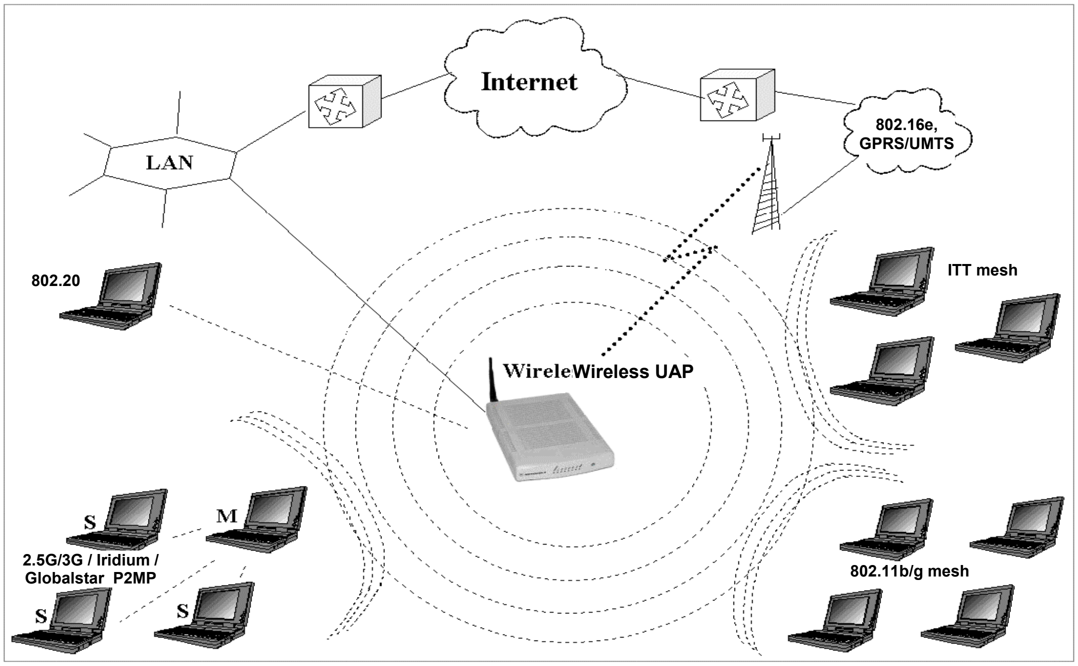


Figure 19. A Universal wireless access point Model[39]

It should be noted that the simple analogy given above does not adequately imitate or address all the functions desired in a wireless UAP. For instance, it does not address what the UAP (the translator in the analogy) must do to prevent wireless devices (the attendees) operating on different frequencies (i.e., speaking different languages) or outside the transmission/reception range of other devices from transmitting (talking) when another device is communicating with the UAP. Nor does it replicate how the UAP would broadcast (speak simultaneously to everyone) messages intended for all wireless devices associated with it. These are all functions a UAP should posses and subsequent paragraphs expound on means of achieving such capabilities.

## A. INTELLIGENT ANTENNA SYSTEM

One of the more difficult obstacles in designing an UAP is enabling it to communicate with mobile and fix wireless devices built on several different wireless standards. As stated earlier, the UAP should possess the capacity to receive and transmit

[39] After: Omar Abuelma'atti, Madjid Merabti, and Bob Askwith, *Interworking the Wireless Domain*, Liverpool John Moores University, http://www.scit.wlv.ac.uk/~jphb/cp4040/rolandonotes/CSNDSP2002/Papers/J1/J1.1.pdf, Last accessed 15 Jan 06.

across the full range of supported licensed and unlicensed wireless radio frequency bands. It should also possess the ability to receive and transmit radio signals of different modulations and spread spectrum technologies over multiple channels concurrently (or near simultaneously). This capability could be achieved with the implementation of an intelligent antenna system. In this context, the definition of such an antenna system is a system of antenna arrays with intelligent signal processing algorithms that are used to identify and remember the frequency of the signal, the modulation/spread spectrum technique used, and the channel of the signal for the device(s) it is communicating with. In other words, an intelligent antenna system has all the capacity needed to emulate the standard transceivers of all the supported wireless standards, giving it the ability to receive and transmit traffic to all the heterogeneous wireless devices in its covering range. This could be accomplished either with a set of multiple transceivers with associated wireless access controllers (those of all the supported standards) or with one or more multi-functioning transceiver. With this capacity, the intelligent antenna system enables the UAP to establish a routing table of devices' interface types, MAC addresses, and IP addresses. The "interface type" is the identification of the 802 wireless standard each wireless device used to establish communication (authenticate and associate) with the UAP. By knowing the devices' interface types, the UAP can determine the correct frequency protocol to use when transmitting traffic to a device that is using a different standard than the device that initiated the traffic. The UAP should also be equipped with a standard Ethernet controller for LAN connectivity and optionally a 2.5G or 3G transceiver such as General Packet Radio Service (GPRS)[40] or Universal Mobile

[40] **G**eneral **P**acket **R**adio **S**ervice is a 2.5G *(*second and a half generation) standard for mobile data service available to users of GSM (Global System for Mobile Communications) mobile phones which runs at speeds up to 115 kilobits per second, compared with current GSM systems' 9.6 kilobits. GPRS is particularly suited for sending and receiving small bursts of data, such as e-mail and Web browsing and large volumes of data, The Free Encyclopedia, http://en.wikipedia.org/wiki/General_Packet_Radio_ Service, Last accessed 17 Feb 06.

Telecommunications System (UMTS)[41] transceiver for future connectivity into the cellular network.[42] Figure 20 below depicts the general architecture for a universal wireless access point.

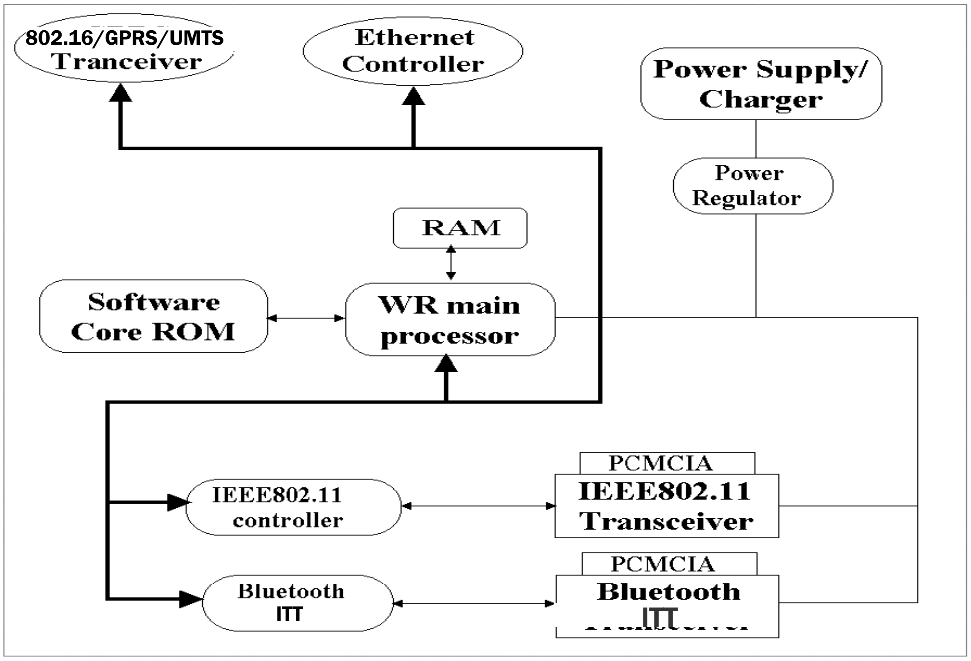


Figure 20. Universal wireless access point Architecture[43]

## B. PROTOCOL BRIDGING SYSTEM (802.X TO 802.Y BRIDGING)

As described in Chapter II of this thesis, one of the challenges that arise in interoperability among different wireless technologies is the problem of protocol mismatch – incompatible layer 2 (L2) protocols used in the heterogeneous devices. To address this problem what's needed is a universal L2 protocol for unified L2 processing[44] or the ability to bridge, through either translation or encapsulation, between different L2 protocols. Since a unified L2 protocol implies the convergence of existing wireless

[41] Universal Mobile Telecommunications System (UMTS) is a 3G (third-generation) mobile technology that supports data transfer rates at speeds up to 2 Mbits/sec. Besides voice and data, UMTS will deliver audio and video to wireless devices anywhere in the world through fixed, wireless and satellite systems. Webopedia, http://www.webopedia.com/TERM/U/UMTS.html, Last accessed 17 Feb 06.

[42] Omar Abuelma'atti, Madjid Merabti, and Bob Askwith.

[43] After: Ibid.

[44] Ramon Aguero and others, *Multi-Radio Access in Ambient Networks*, Wireless World Initiative Whitepaper and Presentation, 08 Nov 05.

standards, conversion via translation or encapsulation appears to be more feasible for a near term solution. Tao, Bochmann, and Dssouli suggest that to solve the problem of protocols mismatch, "a modified version of the transport layer protocol should be implemented in the mobile host and protocol conversion is necessary at the base station."[45] Thus, a UAP should possess the capability to convert heterogeneous source technologies protocols into a generic network protocol and to translate this generic network protocol into the appropriate heterogeneous destination technology protocol.[46] A more succinct approach would be for the UAP to convert the heterogeneous source technologies protocols directly into the appropriate heterogeneous destination technology protocol, without translation into a generic network protocol. No matter which approach is chosen, the UAP must possess the ability to bridge (i.e., convert), either through translation or encapsulation, between different L2 protocols. Depicted in Figure 21 below is a pictorial representation of an 802.x to 802.y wireless bridging operation (where x and y represent different wireless technologies) accomplished through the use of conversion.

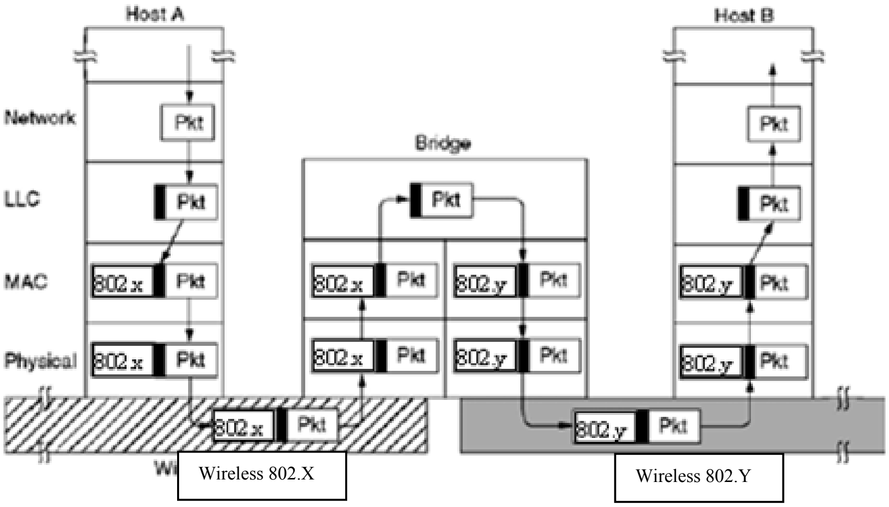


Figure 21. Operation of Wireless Bridging from 802.x to 802.y[47]

[45] Zhongping Tao, Gregor V. Bochmann, and Rachida Dssouli, *A Formal Method for Synthesizing Optimized Protocol Converters and its Application to Mobile Data Networks*, Mobile Networks and Application 2, Baltzer Science Publishers, 1997, 259.

[46] Upkar Varshney, *Network Access and Security Issues in Ubiquitous Computing*, George State University, http://weatherhead.cwru.edu/pervasive/Paper/UBE%202003%20-%20Varshney.pdf, Last accessed 03 Jan 06, 2.

[47] After: Iowa State University, slide 52.

Conversion implies the ability to control how data is forwarded by negotiating existing data translation/encapsulation mechanisms and specifying data payload formats in order to ensure interoperability between different network technologies. In the article "*Protocol Conversion*," Green discusses some examples of specific conversion techniques that have been variously successful as well as the problem of not having a general theory for synthesizing protocol conversions.[48] Tao, Bochmann, and Dssouli also spoke of several formal methods for protocol conversion, which they classify in one of two classes: the bottom–up method and the top-down method. Though they favor the top-down method, they propose an approach that entails generating an optimized converter to overcome some of the top-down method's limitation. [49] Although it is not the intent of this thesis to discuss protocol conversion algorithms, the aim of the preceding statements on this topic were to reveal the feasibility of using such algorithms in a UAP to assist in achieving interoperability between heterogeneous wireless devices and networks.

## C. SOFTWARE DEFINED RADIO TECHNOLOGY

Another state-of-the-art concept that would greatly augment the design of the definitive UAP is that of one of the newest, emerging technology concept, the software defined radio (SDR). For the UAP the SDR enhances the goal of supporting many different standards and technologies by providing a common radio architecture. This is easily understood by viewing a few definitions of a SDR. The Software Defined Radio Forum defines a SDR as:

> a collection of hardware and software technologies that enable reconfigurable system architectures for wireless networks and user terminals. SDR provides an efficient and comparatively inexpensive solution to the problem of building multimode, multi-band, multifunctional wireless devices that can be adapted, updated, or enhanced by using software upgrades.[50]

[48] Paul E. Green Jr., *Protocol Conversion*, IEEE Transactions on Communications, Vol. Com-34, No. 3, Mar 86.

[49] Tao, Bochmann, and Dssouli, 260-266.

[50] Software Defined Radio Forum, SDR Brochure, http://www.sdrforum.org/sdr_brochure_10_24_02.pdf, Last accessed 17 Jan 06.

In a more elaborating interpretation that depicts the significance of a SDR on a UAP design more clearly, McCarthy describes a SDR as:

> a communications device whose operation from the physical layer through higher-level protocol layers is principally defined in software. It supports multiband-multimode radios, global roaming, runtime reconfigurability and over-the-air-programming, alleviating issues arising with the deployment of new communications standards. SDR provides the flexibility of changing a radio's operational ability simply by changing the software code in the device's processing hardware. [51]

In consideration of the above definitions, the ideal UAP built on SDR technology would possess the ability to update or completely change the features of the device by simply uploading new software.[52] With this type of technology, instead of replacing the UAP whenever a new wireless standard is published or new wireless technology developed, the UAP can simply be updated/upgraded with new software patches or service packs as needed. Further increasing the technology's value to the design of a UAP, the SDR has additional benefits such as improving spectrum utilization. Hickling stated that:

> According to the Federal Communications Commission (FCC), "In a software-defined radio (SDR), functions that were formerly carried out solely in hardware, such as the generation of the transmitted signal and the tuning and detection of the received radio signal, are performed by software that controls high-speed signal processors."[53]

Also according to Hickling,

> The SDR Forum goes a step further by defining the ideal SDR as one that has transceivers that perform upconversion and downconversion between baseband and the RF carrier itself exclusively in the digital domain, reducing the RF interface to a power amplifier in the transmit path, a low noise amplifier in the receive path, and little or no analog filtering.[54]

[51] Darren McCarthy, *Software-defined Radio: Integration for Innovation*, RFDesign, Sep 05, 44, http://rfdesign.com/mag/0509RFDF4.pdf, Last accessed 17 Jan 06.

[52] Ronald M. Hickling, *New Technology Facilities True Software-defined Radio*, RFDesign, Apr 05, 18, http://rfdesign.com/mag/504rfdf1.pdf, Last accessed 17 Jan 06.

[53] Hickling.

[54] Ibid.

What this mean is that built on the ideal SDR concepts, the UAP's software can be used to act as an interpreter between completely incompatible radio frequencies and modulation techniques. With such software, the UAP could seamlessly enable a 2.4 GHz device to talk to a 3.5 GHz device, and a device using any version of OFDM to talk to a device using DSSS or QDMA.[55] Figure 22 illustrates a SDR architecture.

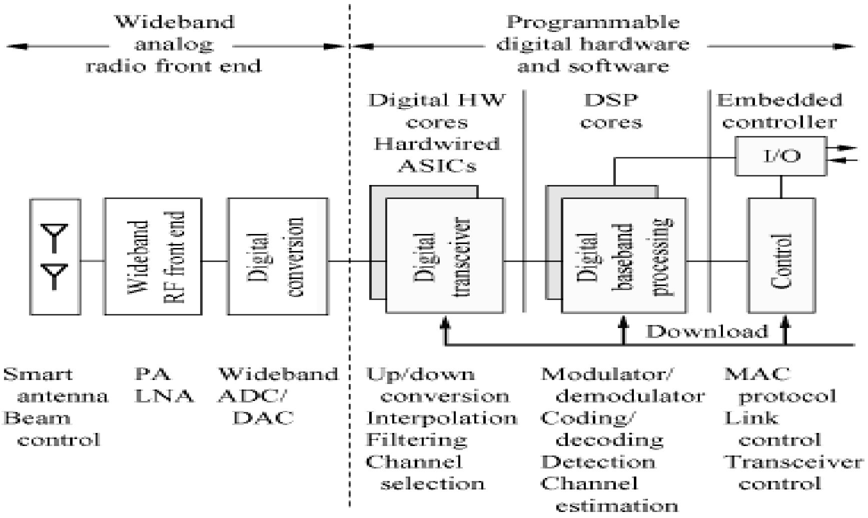

Wideband analog radio front end
Programmable digital hardware and software
Digital HW cores Hardwired ASICs
DSP cores
Embedded controller
I/O
Wideband RF front end
Digital conversion
Digital transceiver
Digital baseband processing
Control
Download
Smart antenna Beam control
PA LNA
Wideband ADC/ DAC
Up/down conversion Interpolation Filtering Channel selection
Modulator/ demodulator Coding/ decoding Detection Channel estimation
MAC protocol Link control Transceiver control

Figure 22. A Software Defined Radio (SDR) Architecture[56]

[55] Hickling.

[56] From: P. R. Chevillat and W. Schott, Broadband Radio LANs and the Evolution of Wireless Beyond 3G, IBM Journal of Research and Development, Volume 47, Number 2/3, March/May 2003, International Business Machines Corporation, 34.

THIS PAGE INTENTIONALLY LEFT BLANK

# IV. IDENTIFICATION OF SOLUTION SETS

## A. IDENTIFICATION OF POSSIBLE COTS/GOTS SOLUTIONS

In reference to the requirements outlined in Chapter III (Definitions, Requirements, and Specifications for a Universal Wireless Access Point), our research uncover several potential solutions, to which some are currently available for implementation, that satisfies some, if not all, of those requirements. The more favorable COTS and/or GOTS technologies discovered were 1) InMotion Onboard Mobile Gateway (oMG) 1000, 2) Netgear Mobile Broadband Router (MBR) 814, 3) Vanu Software Radio GSM Base Station, and 4) Cisco Integrated Services Router – Cisco 2811. Not listed are technologies that have promising potential in the area of UWAP development, but are not ready for implementation. These and similar technologies will be addressed in later chapters.

### 1. InMotion Onboard Mobile Gateway (oMG) 1000

The InMotion Onboard Mobile Gateway 1000 is constructed in a ruggedized case suitable for harsh/remote mobile environments (as seen in Figure 23). This device/access point is designed to accommodate Ethernet, WiFi, 3rd generation (3G) cellular networks (e.g., Verizon, Sprint), and future 4th generation (4G) wireless networks to include 802.20. In addition, peripheral devices (e.g., printers, scanners, etc.) can integrate with it through an integration hub like relationship. Likewise, this technology can act as a WiFi AP or be used as a conduit for WWAN backhaul communications. For mobile applications, the oMG 1000 can receive power from a DC power source (vice using AC power when in stationary/indoor settings). More specifically, this piece of equipment can:

- Operate with WiFi certified client devices (Intel Centrion Certified)
- Support all client operating systems
- Support different peripheral devices through standard WiFi interfaces, Bluetooth, UWB (802.16 and 4G/802.20), USB, Ethernet and Serial interfaces.
- Integrate with current WAN standards including GPRS, GPRS EDGE, UMTS, UMTS TDD (IP Wireless), and Flash-OFDM (Flarion).

- Provide Transparent "Vertical Handoff" Technology
- Supports 254 concurrent users
- Utilize various power inputs (i.e., AC, DC)
- Remote software updates
- 20 Gig storage[57]

Additionally and in accordance with InMotion's OnBoard Mobile Gateway 1000 data sheet, future iteration of this device will allow it to be compatible with new wireless standards such as HSDPA[58], WiDEN[59], and UMTS.[60]

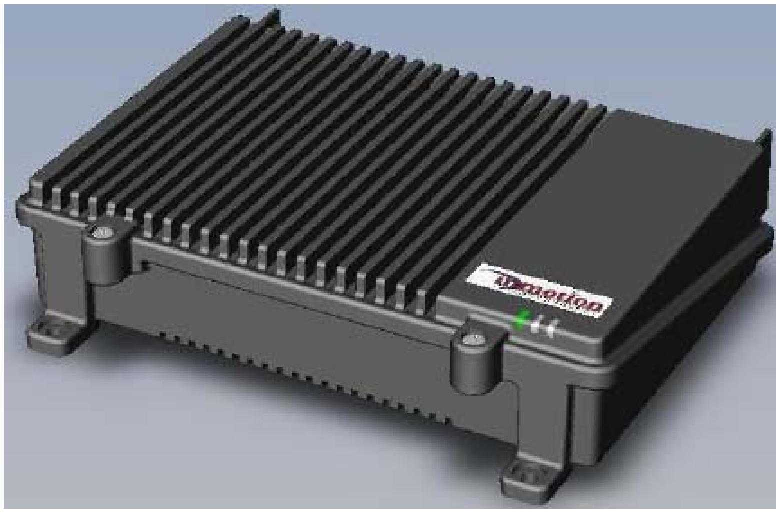


Figure 23. InMotion Onboard Mobile Gateway 1000[61]

[57] InMotion Technology, *Mobile LAN: Enabling Applications on the Edge*, An InMotion Whitepaper 2005, 5-11 and 16.

[58] High Speed Downlink Packet Access (HSDPA) – A packet based data service feature of the in WCDMA standard which provides a downlink with data transmission up to 8-10 Mbps over a 5MHz bandwidth in WCDMA downlink. The high speeds of HSDPA are achieved through techniques including; 16 Quadrature Amplitude Modulation (QAM), variable error coding, and incremental redundancy.

[59] Wideband iDEN – A software upgrade developed by Motorola for its iDEN enhanced specialized mobile radio (or ESMR) wireless telephony protocol. WiDEN allows compatible subscriber units to communicate across four 25 kHz channels combined, for up to 100 kbit/s of bandwidth. The protocol is generally considered a 2.5G wireless cellular technology.

[60] OnBoard Mobile Gateway, *Mobile WLAN: The Next Generation Wireless Platform for Public Safety,* http://www.inmotiontechnology.com/oMG%201000%20Data%20Sheet.pdf, Last accessed 10 Feb 06.

[61] Ibid.

### 2. Netgear Mobile Broadband Router (MBR) 814

The Netgear's MBR 814 design is similar to that of an office or static based routers/access points. However, unlike the typical desktop AP, its design has modularity built into it. As seen in Figure 24 (rear view), the interface to one wireless technology is built-in while the other wireless technology interfaces through a common PCMCIA slot. This architecture may prove beneficial in future applications (for example, later version may support other wireless technologies such as 802.16, etc.). Similar to InMotion's oMG 1000, Netgear's MBR 814 addresses some of the same concerns and offers some of the same capabilities. One similarity is the integration of FLASH-OFDM (comparable FPC card) and 802.11 (built-in) into one box. In addition, this device can support:

- Broadband modem, router, switch and firewall functionality
- Real-time Mobile Interactive and Multimedia applications (most Internet applications)
- Optional special purpose/high gain antennas
- Different interfaces (i.e., WiFi (built-in), FLASH-OFDM, and Ethernet)
- 253 personal computers
- Auto Sensing and Auto Uplink LAN Ethernet connections
- Data rates up to 100 Mbps
- Restriction of MAC addresses
- Full/Half-duplex operations
- Routing Information Protocols (RIP)
- Universal Plug and Play (UPnP)
- Remote management
- Various power inputs (i.e., AC, DC, UPS battery packs)[62]

[62] NETGEAR, Inc., *Reference Manual for the Mobile Broadband Router (MBR) 814*, Netgear, Inc. 2005, 17-23.

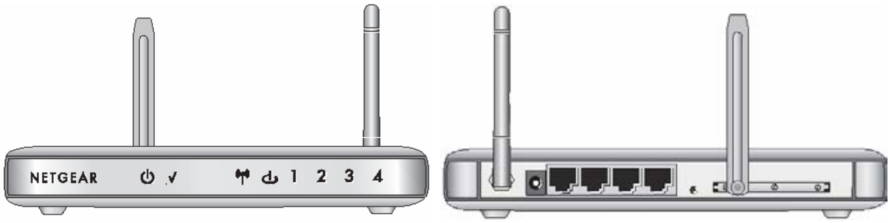


Figure 24. Netgear Mobile Broadband Router (MBR) 814[63]

### 3. Software Radio GSM Base Station

Vanu Inc., along with HP, has taken the SDR concept and implemented it into the first commercially available device termed the Software Radio GSM Base Station – sometimes referred to as the "Anywave Base Station." This device has the ability to "support multiple cellular wireless networks and standards entirely in software."[64] The architecture behind this product is made up of 3 COTS basic building blocks: the antenna subsystem, RF wide band transceiver, and the RF processing platform. The Base Station Transceiver (BTS) and Base Station Controller (BSC), which falls under the RF transceiver and processing platform, are both software radio applications running on an industry standard HP server.[65]

Interoperability wise, the Anywave BS works with a range of third-party backhaul solutions to include fiber, Ethernet, Microwave, Satellite, T1, cable modem and DSL. Additionally, contrary to traditional SDR applications, the Anywave BS can define and perform signal processing through software operations that supports communication between cellular and other wireless devices. Other benefits include:

- Simultaneous support for multiple wireless standards
- Reduced operating expenses
- Ability to add capacity simply by adding a server, and ability to dynamically shift capacity between standards to meet current demand
- Simple, cost-effective migration path to new standards

[63] From: NETGEAR, Inc., pages 21-22.

[64] Vanu Software Radio, *Addressing the Complexities of Software Defined Radio (SDR)*, http://h71028.www7.hp.com/enterprise/downloads/SDR_SolutionBrief.pdf, Last accessed 09 Feb 06.

[65] VANU, *The Anywave Base Station*, http://vanu.com/products/basestation.html, Last accessed 12 Feb 06.

- Simultaneously support combinations of GSM/GPRS, EDGE, CDMA, 3G and 4G standards
- Support a myriad of circuit switch, packet and multimedia services
- Allows for other innovative capabilities such as remote network monitoring
- Can integrate with either a legacy MSC switch configurations or the new generation of emerging soft switches[66]

To clarify why Vanu's Anywave Base Station is deemed a SDR and what additional capabilities it provides because its a SDR the following information is provided. A device that uses software in place of hardware to perform signal processing using application-level software is in the Software Defined Radio (SDR) technology arena. As eluded to above, this is one of the many capabilities of the Anywave Base Station. This technology, SDR, is on the cutting edge of revolutionizing how we communicate wirelessly. Architectures built on this concept are "an enabling technology that is applicable across a wide range of areas within the wireless industry." Additionally, the following data points are characteristics of SDRs and thus also characteristics of the Anywave Base Station:

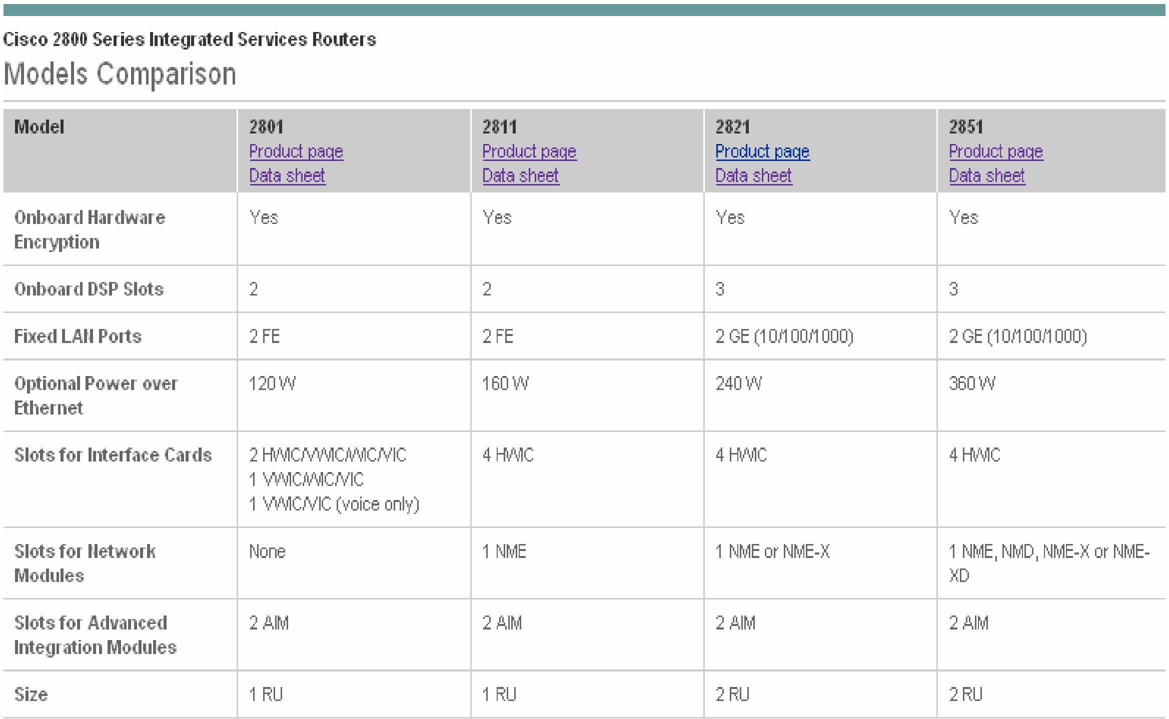
- Open Standards and flexible architectures for a wide range of communications products.
- Enhanced wireless roaming for consumers by extending the capabilities of current and emerging commercial air-interface standards.
- Over-the-air downloads of new features and services as well as software patches.
- Advanced networking capabilities to allow truly portable networks.
- Unified communication across commercial, civil, federal, and military organizations.
- Significant life cycle cost reductions.[67]

[66] VANU, *Vanu, Inc Announces the First Commercial Software Radio Deployment in Canada*, http://vanu.com/news/prs/ICEWirelessFinal.pdf, Last accessed 12 Feb 06.

[67] PRISMTECH, *Software Defined Radio SDR*, http://www.prismtechnologies.com/section-item.asp?sid4=&sid3=&sid2=6&sid=17&id=73, Last accessed 12 Feb 06.

### 4. Integrated Services Router – Cisco 2811

The Cisco 2800 series integrated services routers (2801, 2811, 2821, and 2851) are a spin off from the 2600 series. According to manufacture specifications, this series supports Layer 2 switching with Power over Ethernet (PoE), high-density serial connectivity, enhanced network analysis, and traffic management tools. These routers also offer such improvements as embedded security processing and new high-density interfaces. The high-density interfaces in particular, heighten the performance, availability, and reliability required for scaling missions. In addition, Cisco 2800 series routers have functionality that support wireless LANs. Specifically, they support WLAN coverage, providing wireless capabilities combined with routing and security features in a single device.[68] See Table 1 for model comparisons.



Cisco 2800 Series Integrated Services Routers

Models Comparison

| Model | 2801<br>Product page<br>Data sheet | 2811<br>Product page<br>Data sheet | 2821<br>Product page<br>Data sheet | 2851<br>Product page<br>Data sheet |
|---|---|---|---|---|
| Onboard Hardware Encryption | Yes | Yes | Yes | Yes |
| Onboard DSP Slots | 2 | 2 | 3 | 3 |
| Fixed LAN Ports | 2 FE | 2 FE | 2 GE (10/100/1000) | 2 GE (10/100/1000) |
| Optional Power over Ethernet | 120 W | 160 W | 240 W | 360 W |
| Slots for Interface Cards | 2 HWIC/WIC/VIC/VIC<br>1 VWIC/WIC/VIC<br>1 VWIC/VIC (voice only) | 4 HWIC | 4 HWIC | 4 HWIC |
| Slots for Network Modules | None | 1 NME | 1 NME or NME-X | 1 NME, NMD, NME-X or NME-XD |
| Slots for Advanced Integration Modules | 2 AIM | 2 AIM | 2 AIM | 2 AIM |
| Size | 1 RU | 1 RU | 2 RU | 2 RU |

Table 1. Cisco 2800 Series Integrated Services Routers Model Comparison[69]

[68] Miercom Lab Testing Summary Report, http://www.cisco.com/application/pdf/en/us/guest/products/ps5854/c1244/cdccont_0900aecd8017382b.pdf, Report 040903, September 2004, Last accessed 21 Feb 06.

[69] From: Cisco Systems, Model Comparison, http://www.cisco.com/en/US/products/ps5854/prod_models_comparison.html, Last accessed 21 Feb 06.

One of the key factors that make this device a viable UWAP solution is its modularity and customization capabilities. Although each of the 2800 series routers posses some degree of modularity, the Cisco 2811 router (displayed in Figure 25) is optimum because it exhibits the required functionality and is the most cost effective.

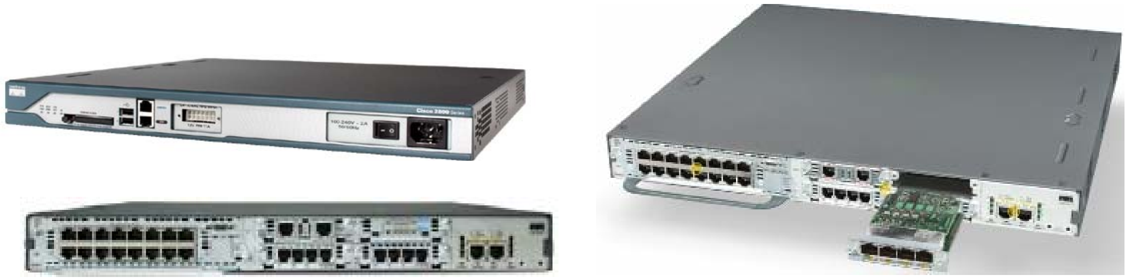


Figure 25. Cisco 2811 Router and Cisco 2811 with HWIC extracted.[70]

The Cisco 2811 supports the following functions, which makes it a more robust device than its predecessor, the Cisco 2600 series router.

- Wire-speed performance for concurrent services such as security and voice , and advanced services to multiple T1/E1/xDSL WAN rates
- Enhanced investment protection through increased performance and modularity
- Enhanced investment protection through increased modularity
- Increased density through High-Speed WAN Interface Card Slots (four)
- Enhanced Network Module Slot
- Support for over 90 existing and new modules
- Support for majority of existing AIMs, NMs, WICs, VWICs, and VICs
- Two Integrated 10/100 Fast Ethernet ports
- Optional Layer 2 switching support with Power over Ethernet (PoE) (as an option)
- Security:
    - On-board encryption
    - Support of up to 1500 VPN tunnels with the AIM-EPII-PLUS Module

[70] From: Cisco Systems, *Cisco System Integrated Service Routers*, http://www.cisco.com/cdc_content_elements/flash/nextgen/webversion/portfolio/demo.htm?NO_NAV, Last accessed 21 Feb 06.

- Antivirus defense support through Network Admission Control (NAC)
  - Intrusion Prevention as well as stateful Cisco IOS Firewall support and many more essential security features
- Voice:
  - Analog and digital voice call support
  - Optional voice mail support
  - Optional support for Cisco Call Manager Express (Cisco CME) for local call processing in stand alone business for up to 36 IP Phones
  - Optional support for Survivable Remote Site Telephony support for local call processing in small enterprise branch offices for up to 36 IP phones.[71]

## B. COMPARATIVE ANALYSIS OF IDENTIFIED POTENTIAL COTS/GOTS SOLUTIONS

This section provides a visually intuitive comparison chart and identifies several pros and cons of the various technologies/devices mentioned earlier in this chapter. Important to note is that only those functionalities remotely critical to the operations of a UAP are listed under the "Capability" column in Table 2 below. The full spectrum of capabilities offered by these devices/technologies is accessible by viewing their perspective device manuals and/or web sites. Intentionally excluded from this table are those devices/ technologies that are still in their concept or developmental stages. However, subsequent chapters will identify those technologies that are currently in development that may prove beneficial towards future advancements concerning a Universal Wireless Access Point (UWAP).

| **CAPABILITY** | **INMOTION<br>Onboard Mobile Gateway 1000** | **NETGEAR<br>Indoor Desktop Modem/Bridge** | **VANU<br>SDR GSM Base Station** | **CISCO<br>2811<br>Router** |
|---|---|---|---|---|
| Modularity | Yes<br>PCMCIA Slot(s): 1 | Yes<br>PCMCIA Slot(s): 1 | No | Yes<br>(4 HWIC slots) |
| Environment | Mobile / remote (ruggedized case) | Mobile (desktop quality) | Mobile | Static |
| Functionality | Supports | Supports | Supports voice | Supports data |

[71] Cisco Systems, Cisco 2811Integrated Services Router, http://www.cisco.com/en/US/products/ps5881/index.html, Last accessed 21 Feb 06.

| | | | | |
|---|---|---|---|---|
| | broadband data and voice. | broadband data and voice | (cellular) | and voice |
| Interfaces | WiFi (built-in), Bluetooth, FLASH-OFDM, USB, Ethernet, Serial, 3G cellular networks | WiFi (built-in), FLASH-OFDM, and Ethernet | Fiber, Ethernet, Microwave, Satellite, T1, cable modem, 3G cellular networks, DSL | Ethernet, high-density serial, T1, E1, USB, DSL, WiFi (built-in or via HWIC module) |
| Intelligent Antenna System | Multiple Antennas (dual) | Multiple Antennas (dual)<br>Optional Special Purpose/ High-Gain Antennas | Yes | Field-Replaceable Optional High-Gain Antennas Diversity (dual) Antennas |
| Protocol Conversion Enabled | Yes<br>IEEE 802.11b/g, FLASH-OFDM 802.20, IEEE 802.3, IEEE 802.15, IEEE 802.16e | Yes<br>IEEE 802.11g, FLASH-OFDM 802.20, IEEE 802.3 | Yes<br>Simultaneous support for multiple wireless standards (voice), 802.3 | Yes<br>IEEE 802.11b/g, IEEE 802.3 |
| SDR Enabled | No | No | Yes | No |
| Utility | WiFi AP or WAN backhaul | WiFi AP or WAN backhaul | Integrate cellular technologies | Router / AP Functionality |
| Wireless Standards Supported | GPRS, GPRS EDGE, UMTS, UMTS TDD (IP Wireless), 802.11, 802.15, 802.16 and 802.20 | 802.11 and 802.20 | GSM/GPRS, EDGE, CDMA, 3G cellular | 802.11 |
| Other | Provide Transparent “Vertical Handoff” Technology<br>Remote software updates capability | Broadband modem, router, switch, and firewall functionality.<br>Real-time Mobile Interactive and Multimedia applications. (most Internet applications) | Perform signal processing through software operations which supports communication between cellular and other wireless devices | |

Table 2. Solution Comparison Chart.

In accordance with Table 2 above, the following paragraphs summarize the advantages or disadvantages of each particular device. The first two technologies mentioned below, at their present maturity level, failed to meet the minimal requirements needed in the deployment of a universal wireless access point. Conversely, the latter two devices/technologies, though lacking some desired functionality, demonstrated the most potential.

### 1. Vanu "Anywave Base Station"

Though our review did not comprise every commercially available SDR system, of the countless systems reviewed, the Anywave Base Station was the only device that exhibited technology mature enough to be considered as a candidate solution for a UAP. However, in spite of the remarkable achievements by Vanu in the SDR arena, the Anywave Base Station falls short of meeting TNT environmental utility. Though the concept of SDR introduced by Vanu is headed in the right direction, the Anywave Base Station is focused primarily on cellular (voice) type applications and not enough on data streaming (e.g., video, data) networks similar to that found within TNT operations.

Equally, DoD also attempted to field a SDR prototype called JTRS (Joint Tactical Radio System) (pronounced Jitters) that would provide more utility in an all services urban terrain environment. Unfortunately, this system is still in its developmental stages. Though JTRS will replace the majority, if not all of the military radio communication systems currently in uses, future research will be required once the system is completed and fielded to assess its full capabilities.

### 2. Cisco "2811"

As identified in the capabilities section listed above, the 2811 has four High-Speed WAN Interface Card (HWIC) slots as seen in Figure 25 above. The four HWIC slots can accommodate any arrangement of WAN or Voice Interface Cards (HWICs, WICs, VWICs, or VICs) as well as double wide HWIC-Ds. Additionally these HWIC slots can house modified versions of PCMCIA cards (Figure 26 below) to give the 2811 access point functionality. This degree of modularity separates the Cisco 2811 router from other models. Because of this uniqueness, this device could play a potentially critical role in developing joint "universal" access point technology that can communicate with several wireless node using different technologies. However, to date this device can only accommodate 802.11 PC cards, which is an inhibitor to expanding TNT operations were various wireless technologies are operating simultaneously.

Figure 26. Cisco HWIC AP.[72]

### 3. Netgear "MBR 814" and InMotion "oMG 1000"

Both the Netgear Mobile Broadband Router (MBR) 814 and the InMotion Onboard Mobile Gateway (oMG) 1000 are designed to incorporate the FLASH-OFDM technology. However, in addition to that, what makes both of these devices particularly important to the designing of a UAP is: 1) their modularity capabilities and 2) they already posses the ability to incorporate at least two of the current wireless technologies used within TNT experimentations (802.11b/g and 802.20).

#### *a. Modularity Capability*

As mentioned, both devices currently operate using 802.11 and 802.20 technologies all in one device. At present, both devices use 802.11 to communicate with neighboring wireless nodes that house an equivalent PC card and the 802.20 is used as a conduit for backhaul connectivity. As seen in Figure 24 above (Netgear's MBR 814 rear view) and in Figure 27 below (InMotion's oMG 1000 inside view), both devices has the ability to accommodate various wireless cards. Future test will reveal if either device is able to use 802.20 to communicate with wireless nodes outfitted with 802.20 wireless cards in conjunction with using 802.20 for backhaul communications.

[72] From: Cisco System, *Wireless Services on the Cisco 800, 1800, 2800, and 3800 Series Integrated Services Router Date Sheet,* http://www.cisco.com/application/pdf/en/us/guest/products/ps5854/c1650/cdccont_0900aecd8016ef57.pdf, Last accessed 25 Jan 06.

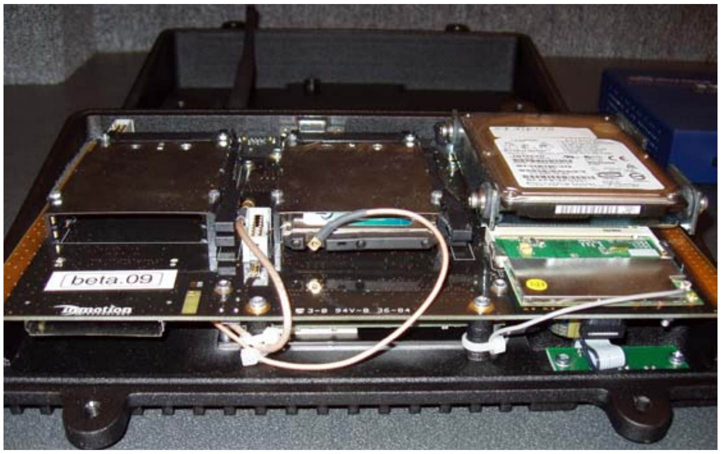


Figure 27. InMotion Onboard Mobile Gateway 1000 (inside view)

#### *b. Wireless Technologies Conversion Capability*

One of the main functionality identified in the capabilities of a UAP is the ability to conduct protocol conversions between neighboring technologies (e.g., 802.11, 802.16, 802.20, etc,) and ultimately to 802.3 Ethernet. Netgear and InMotion has been able to master at least two of these (802.11 and 802.20) to a certain degree. Having already paved the way by developing the algorithmic conversions necessary for these two technologies, including others are well within their reach. Similarly, future test will determine the extent of their capabilities in this area.

The FLASH-OFDM component in the Netgear's MBR 814 and InMotion's oMG 1000 plays an integral part in their ability to do protocol conversion. Additionally, unlike other wireless technologies, FLASH-OFDM technology, manufactured by Flarion Technologies, is a mobile broadband system designed to allow typical WAN communications to operate in a cellular environment. As mentioned in chapter 2, OFDM is one of several different modulation/ spread spectrum technologies used within wireless networks. More specifically, according to recent research conducted by William J. Parish and Daniel R. Tovar, OFDM is:

> …a multi-carrier approach that segments according to frequency and therefore divides spectrum into equally spaced tones. Each tone will contain a user's information and in conjunction with a multiple access scheme will allow many users to share the frequency.

They continued by stating:

> The benefits of OFDM are realized in its ability to overcome problems often encountered in a wireless environment such as multi-path, time dispersion, Doppler spread, and rayleigh fading.[73]

The FLASH component of FLASH-OFDM is a new signal-processing scheme that has the capability of supporting high data rates at incredibly low packet and latency loss over a distributed all-IP wireless network. As a result, it will enable real-time mobile interactive and multimedia applications.[74]

From a more technical perspective and in accordance with manufacture's specifications, FLASH-OFDM has a vertically integrated design at Layers 1 and 2. However, the remaining protocol layers are horizontally layered. In an IP based environment, this configuration is permissible because only the layers above the data link layer (layers 3 through 7) need to be horizontally layered.[75] What this means is that in spite of the fact that layers 1 and 2 are vertically integrated, this architecture maintains interoperability with pre-existing off-the-shelf IP infrastructure devices and protocols. Figure 28 represents the contrast between Traditional Layering and FLASH-OFDM Layering.

[73] William J. Parish and Daniel R Tovar, 7-9.

[74] CellularOnline, Flash-OFDM (Orthogonal Frequency Division Multiplexing), http://www.cellular.co.za/flash-ofdm.htm, Last accessed 27 Jan 06.

[75] Ibid. 8.

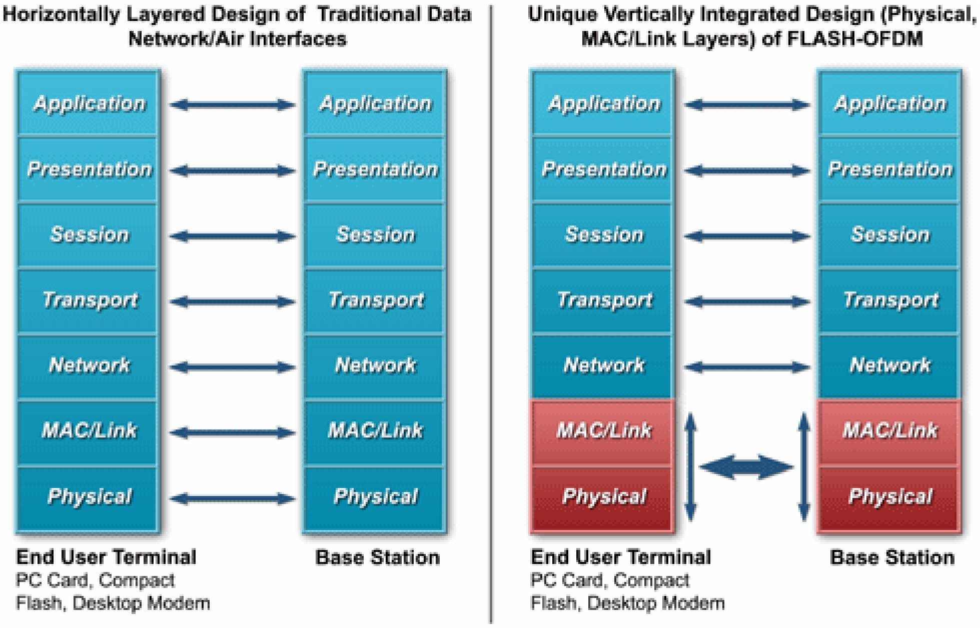

Horizontally Layered Design of Traditional Data Network/Air Interfaces
Unique Vertically Integrated Design (Physical, MAC/Link Layers) of FLASH-OFDM
Application
Presentation
Session
Transport
Network
MAC/Link
Physical
End User Terminal
PC Card, Compact Flash, Desktop Modem
Base Station

Figure 28. Traditional Layering vs FLASH-OFDM Layering[76]

One of the main reasons behind dividing the OSI stack horizontally in the beginning was to "compartmentalize" service layer functionality from its adjacent layers. However, this architecture leads to interoperability limitations when trying to communicate with networks with different structures. In other words, stringent horizontally layered architectures restrict the vertical exchange of data between heterogeneous networks. In efforts to overcome this problem, technologies similar to that used in FLASH-OFDM are coming into fruition.

Referring back to the manufactures specifications and in conjunction with an earlier statement pertaining to an all-IP based wireless network, the FLASH-OFDM system is a packet-switched nationwide system that possess the capability to deliver resilient communications that demonstrates the following characteristics:

- Broadband access - average downlink user data rates of 1 to 1.5 Mbps, with burst rates of 3.2 Mbps; average uplink user data rates of 300-500 kbps, with burst rates of 900 kbps; latency (network delay) below 50 milliseconds

[76] From: Flarion, *FLASH-OFDM Technology*, http://www.flarion.com/products/flash_ofdm.asp, Last accessed 25 Jan 06.

- One wireless wide area network for broadband data and voice
- All-IP and packet-switched: no changes to protocol, settings, devices and content required
- Quality of Service (QoS) for priority access
- Highest spectral efficiency of any mobile broadband system commercially available (only 1.25 MHz paired Frequency Division Duplexing (FDD) spectrum needed for a nationwide network)
- Enterprise-class security
- WLAN - Wireless LAN interoperability (ubiquitous access) with WiFi[77]

[77] Flarion, *The FLASH-OFDM System*, http://www.flarion.com/about/default.asp, Last accessed 04 Feb 06.

THIS PAGE INTENTIONALLY LEFT BLANK

# V. CONCLUSIONS AND RECOMMENDATIONS

## A. RESEARCH CONCLUSION

### 1. Analysis of Problem and Identification of Solution Requirements

The research documented in this thesis first endeavored to identify the current status of interoperability between TNT's wireless network devices and AP/BS and the limitations (problems and challenges) associated with interoperability between the heterogeneous wireless technologies that are used by these devices that make up the wireless networks. Included in the problem set were several major findings, which were grouped into the following three categories:

(1) shortcoming in wireless technology specifications and standards,

(2) differences in frequencies and spread spectrum or modulation techniques implemented in the wireless technology, and

(3) differences in the layer 2 (i.e., data link layer) protocols, specifically the composition, functions, and data frame format of these wireless technologies' data link layer.

With these limitations in mind, this study then moved to identify the functional and hardware requirements necessary to achieve interoperability amongst TNT's heterogeneous wireless networks via a joint (universal) wireless access point (UWAP/UAP). Two major requirements, in addition to those already present in current AP functionalities, were identified: (1) the need for an Intelligent Antenna System and (2) a protocol bridging system for conversion between 802.x and 802.y technologies. A third requirement, functionalities defined in the emerging software defined radio (SDR) technology, was identified as an enhancement to the capabilities desired in a UWAP/UAP rather than a necessity. With the technology to achieve these requirements already a reality or under development, the feasibility of achieving interoperability between heterogeneous wireless networks via a UWAP/UAP was definitely determined to be plausible.

### 2. Potential Solutions Comparative Analysis Conclusion

With the determination that a UWAP/UAP is achievable within the current state of technology, this thesis turned toward the analysis of potential solutions that already existed. During the analysis, several COTS and GOTS devices were evaluated for possible implementation as a universal wireless access point. From this evaluation, four devices were identified as potential solution:

(1) Cisco's 2811 Integrated Services Router with High-Speed WAN Interface Card (HWIC). Equipped with the Cisco HWIC-AP 802.11a/b/g Wireless LAN interface cards, the Cisco 2811 can provide integrated access point functionality as well as rich router services. This combination offers ease of configuration, deployment, and management while delivering high performance, security and a rich set of services. With this configuration, enterprise branch offices and small-to-medium businesses' customers can run concurrent services of Layer 3 routing, security, Layer 2 switching, and IEEE 802.11 wireless LAN functionality from a single platform. The Cisco 802.11 WLAN Interface Card provides Cisco 2811 Integrated Services Routers dual band 802.11a/b/g radios, support for fixed, external dipole or dual mode antennas, extensive WLAN Security Capabilities, and multiple VLAN support.[78]

(2) Netgear's Mobile Broadband Router (MBR) 814. This Wireless Mobile Broadband Router uses the FLASH-OFDM technology for broadband connectivity that supports real-time mobile interactive and multimedia applications. This device has Four 10/100 Ethernet LAN ports to support up to 253 networked computers and a built-in 802.11g wireless access point to extend the network to support up to 32 wireless 802.11b or 802.11g users. The MBR 814 is also equipped with a PC Card slot. This slot contains the Flarion 1000 PC Card to provide reliable, wireless broadband connectivity to an 802.20 base station.[79]

(3) InMotion's Onboard Mobile Gateway (oMG) 1000. This device is a ruggedized edge server and wireless gateway, designed for use in challenging multi-

[78] Cisco Systems, Inc, *Cisco HWIC-AP WLAN Module For Cisco 1800 (Modular), Cisco 2800 And Cisco 3800 Series Integrated Services Routers Data Sheet*, 1995-2000, 1.

[79] NETGEAR, Inc, *MBR14XF 802.11g FLASH-OFDM Mobile Broadband Router*, http://www.netgear.com/pdf_docs/MBR814XF_ds_r2_2Sep05.qxd.pdf, Last accessed 14 Mar 06.

device, multi-application and/or multi-networking environments. The oMG 1000 enables the seamless extension of mission critical information management resources through the convergence of next generation LAN and WAN technologies including Ethernet, 802.11/WiFi, 3rd generation (3G) cellular networks and 4th generation wireless networks including 802.20.[80] The oMG is forward compatible with next generation cellular data technologies such as 1xEV-DO and UMTS and with more recently developed wireless technologies including 802.11a, 802.11g and 802.16 WiMax. Additionally, the oMG is designed in a modular fashion so that both the WLAN and WWAN backhaul components can be upgraded as new technologies become available.[81]

(4) The Software Radio GSM Base Station (aka, Anywave Base Station) prototyped by Vanu Inc. in conjunction with Hewlett Packard. The Anywave Base Station runs on a general-purpose server and a base transceiver station (BTS) and a base station controller (BSC) entirely through software. Thus the signal processing for a range of waveforms is accomplished solely through the use of software. Providing support for new waveforms is accomplished through software downloads, not hardware upgrades. Currently, the Vanu BTS only implements GSM, GPRS, and EDGE functionality. However, the next release of the Anywave Base Station software will provide support for multiple wireless network protocols.[82] It is hoped that 802.11, 802.16, and 802.20 are included in the list of future network wireless protocols.

These devices were evaluated in several critical areas to include their inclusion of an intelligent antenna system, protocol conversion system, wired and wireless interfaces, current support of wireless standards, modularity, and functionalities associated with SDR technology. The device that fared the best from this evaluation was the oMG 1000 produced by InMotion. This device's specifications included the capability to support several of the wireless standards utilized in TNT to include 802.11b/g, 802.16, and 802.20. Additionally, it was discovered through email conversation with Mike Dooley,

[80] InMotion Technology Inc., *Mobile WLAN: The Next Generation Wireless Platform for Public Safety*, 2005.

[81] InMotion Technology Inc., *Mobile LAN: Enabling Applications on the Edge*, 11.

[82] VANU, Anywave Base Station, http://vanu.com/products/basestation.html, Last accessed 12 Feb 06.

Director of Sales for InMotion Technology Inc., that with the development of the proper drivers this device could be modified to support ITT wireless devices. With four built-in PCMCIA slots the oMG 1000 is extremely modular, allowing for easy exchange of wireless interfaces and field upgrade of key components. The next step in evaluating this device suitability for meeting TNT's joint point technology solution requirements is to evaluate its operational performance during future TNT experiments. Our recommendation to integrate this device into TNT's future experiments, as well as a list of devices required to implement a 802.20 network in the TNT environment, are addressed in the following paragraph.

## B. RECOMMENDATIONS FOR FUTURE RESEARCH

Several emerging technologies exhibit enormous potential in the wireless access point arena. Among these, the InMotion oMG 1000 appears to be the most promising, near-term solution to the realization of an UWAP for TNT. Therefore, we strongly recommend further assessment of this device be conducted through additional research and hands-on, operational evaluation of this device in the TNT environment. To facilitate the full evaluation of this device in the TNT environment a 802.20 wireless network needs to be established. To completely construct a wireless FLASH-OFDM, 802.20 wireless, based environment that is capable of interacting with other network and wireless technologies seamlessly, the following devices and components are needed:

- RadioRouter (RR) Base Station (BS) – both a wireless BS and an IP access router (as seen in Figure 12 – Chapter 2)
- Element Management System (EMS) Server – radio access network management system
- Mobile Network Server – assists the RR BS with maintaining mobile connectivity
- Authentication, Authorization, and Accounting (AAA) Server – allows user profiles to be manipulated remotely
- Terminal Equipment – desktop, laptops, and modems/bridges
- FPC 1000 or 2500 PCMCIA or CF Card - manufactured by Flarion, these card captures the two Flarion's concepts, FLASH and OFDM, together and optimizes them to work in what resembles an Ethernet NIC card (Type II PCMCIA) or Compact Flash Card

Concerning a more optimal or ideal solution, the following technologies/concepts are promising: Generic Link Layer Architecture, the Joint Tactical Radio Systems (JTRS) concept, and Control and Provisioning of Wireless Access Point (CAPWAP) Protocol.

### 1. Generic Link Layer (GLL) Architecture

Technologies designed with Generic Link Layer (GLL) functionality have the capability to enhance wireless communications in numerous areas. Some of these capabilities include a unified interface to upper layers and bridging between different L2 (layer 2) protocols[83] as outlined in Chapter 2 of this thesis. See Figures 29 and 30 for examples of GLL layer 2 sub-layers and how they interface with upper and lower layers. In reference to Figure 29, the packet data convergence protocol (PDCP) is responsible for header compression, the radio link control (RLC) is responsible for segmentation and correction of transmission errors, and the MAC sub-layer is responsible for scheduling and priority handling. An important function to note about GLL is its interface link to control and configuration manager as illustrated in Figure 30. This interface addresses radio link layer characteristic that is technology specific and falls outside the standard radio link layer parameters. In such cases, this interface allows additional control and configuration functionality; however, further development is necessary in this area.[84]

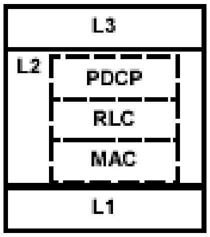


Figure 29. Radio Link Sub-Layers[85]

[83] Ramon Aguero, *Multi-Radio Access in Ambient Networks*, Wireless World Initiative 2005, 8.

[84] Joachim Sachs and others, *A Generic Link Layer for Future Generation Wireless Networking*, http://ieeexplore.ieee.org/iel5/8564/27114/01204448.pdf?arnumber=1204448, 835-36, Last accessed 03 Jan 06.

[85] From: Ibid, 836.

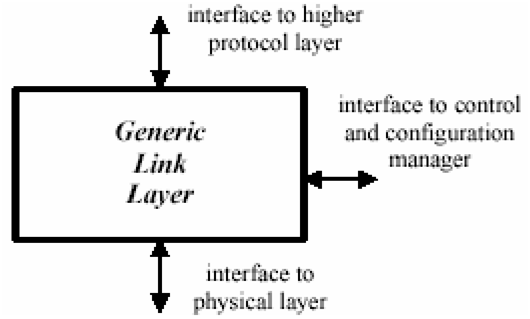

interface to higher protocol layer
Generic Link Layer
interface to control and configuration manager
interface to physical layer

Figure 30. GLL Functions and Interfaces[86]

Additionally, GLL promises to have the capacity to allow resourceful collaboration between different radio technologies in a seamless fashion. What makes this possible is an accessible toolbox of link layer functions, which are configurable to any radio access technology as per their requirements. However, to support a broad spectrum of diverse WLAN PCMCIA cards, a special algorithm is required to identify (dynamically) the different WLAN cards and their particular characteristics. Once identified, the GLL will then implement that link layer functionality. Figure 31 represents the algorithm (flowchart format) which is needed to recognize and/or measure different WLAN PCMCIA cards.

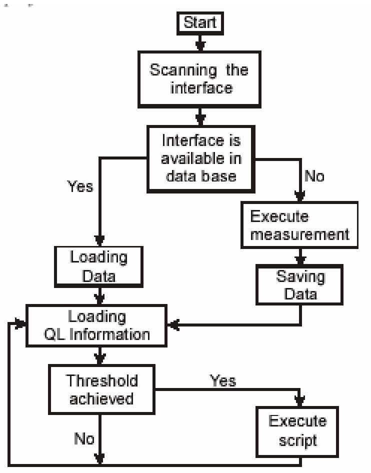
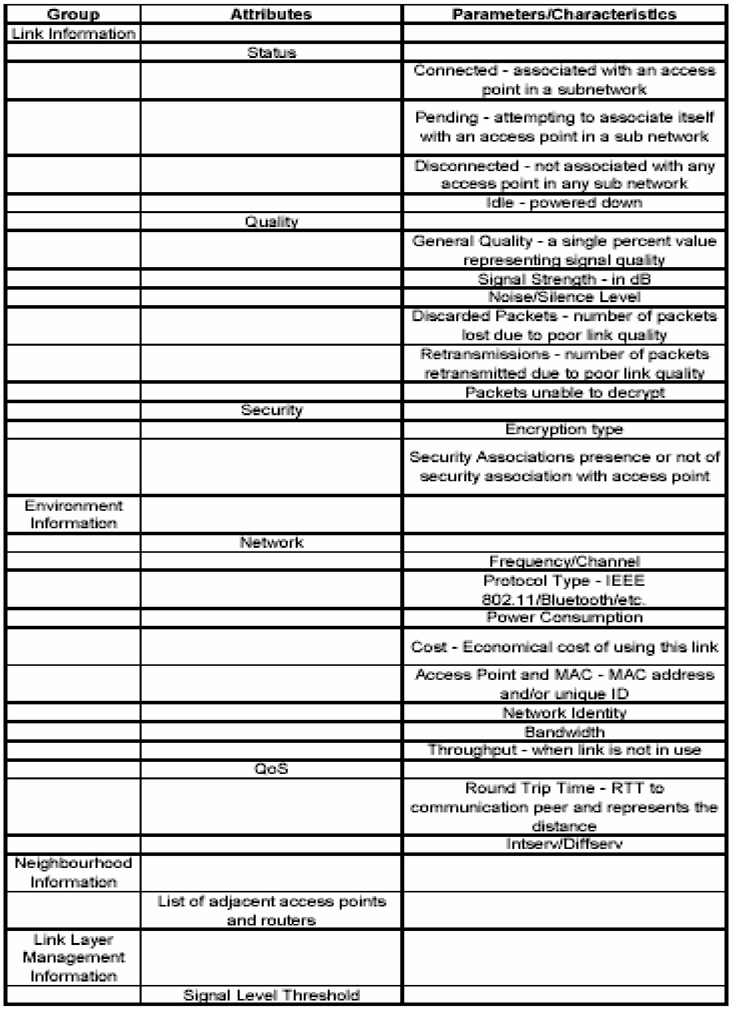


Figure 31. Flow chart of algorithm for WLAN PCMCIA card measurements[87]

[86] From: Joachim Sachs and others, 837.

[87] From: Stefan Aust and others, *Policy Based Mobile IP Handoff Decision (POLIMAND) Using Generic Link Layer Information*, http://www.iponair.de/publications/Aust_MWCN2003.pdf, 3, Lasted accessed 07 Feb 06.

Concerning wireless networks, the link layer functions (parameters) are broken down into four general areas: (1) Link Information – represents the status, quality, and loss characteristics of a single link, (2) Environment Information – provides information on neighboring access points and routers, (3) Neighborhood Information – identifies all access points and respective routers in the vicinity, and lastly (4) Link Layer Management Information.[88] Depicted in Table 3 are examples of these parameters.



| Group | Attributes | Parameters/Characteristics |
|---|---|---|
| Link Information | | |
| | Status | |
| | | Connected - associated with an access point in a subnetwork |
| | | Pending - attempting to associate itself with an access point in a sub network |
| | | Disconnected - not associated with any access point in any sub network |
| | | Idle - powered down |
| | Quality | |
| | | General Quality - a single percent value representing signal quality |
| | | Signal Strength - in dB |
| | | Noise/Silence Level |
| | | Discarded Packets - number of packets lost due to poor link quality |
| | | Retransmissions - number of packets retransmitted due to poor link quality |
| | | Packets unable to decrypt |
| | Security | |
| | | Encryption type |
| | | Security Associations presence or not of security association with access point |
| Environment Information | | |
| | Network | |
| | | Frequency/Channel |
| | | Protocol Type - IEEE 802.11/Bluetooth/etc. |
| | | Power Consumption |
| | | Cost - Economical cost of using this link |
| | | Access Point and MAC - MAC address and/or unique ID |
| | | Network Identity |
| | | Bandwidth |
| | | Throughput - when link is not in use |
| | QoS | |
| | | Round Trip Time - RTT to communication peer and represents the distance |
| | | Intserv/Diffserv |
| Neighbourhood Information | | |
| | List of adjacent access points and routers | |
| Link Layer Management Information | | |
| | Signal Level Threshold | |

Table 3. List of available network parameters[89]

[88] Stefan Aust and others.

[89] From: Ibid.

The main thrust behind adopting GLL architecture into the wireless arena is that it unifies the interface to the network layer. The potential capabilities offered by GLL technology are becoming more and more critical in this world of diversified (heterogeneous) wireless communications.

### 2. Joint Tactical Radio System

The Joint Tactical Radio System (JTRS) (Figure 32 below) is a family of software-programmable tactical radios. They will provide combat personnel with voice, data, and video communications that are interoperable among all battlefield participants regardless of the branch of service. Once it is fielded and becomes fully operational, it will optimize interoperability among not only heterogeneous technologies but also between varying DoD organizations. In addition, all branches of the military will be able to benefit from this technology. The brief list below highlights a few of its capabilities:

- A new, wideband, networked waveform that provides mobile connectivity and access to IP-based information posted on the network across the battle space
- Sufficient bandwidth for voice, data, and video communications
- Compatibility with the 23 waveforms currently in use by the DoD and interoperability between all service branches

Figure 32. JTRS Cluster One[90]

[90] From: Boeing, *Integrated Defense System*, http://www.boeing.com/defense-space/ic/jtrs/index.html, Last accessed 16 Feb 06.

JTRS is designed on top of an architecture call Software Communications Architecture (SCA). This architecture is the key protocol used that enables the functionality and expandability found within JTRS. In accordance with a data sheet published on an Army website, SCA is an open architecture framework that governs how H/W and S/W is to interact within JTRS. The guidelines specified in SCAs are used to manufacture the various components found in what is call JTR sets. These JTR sets consist of several parts: software application waveforms (e.g., Wideband Networking Waveform (WNW)), network services, and the programmable radio set (i.e., the traditional radio box). Figure 33 below shows the relationship of several JTR sets are networked together, which at that point forms a JTRS.[91]

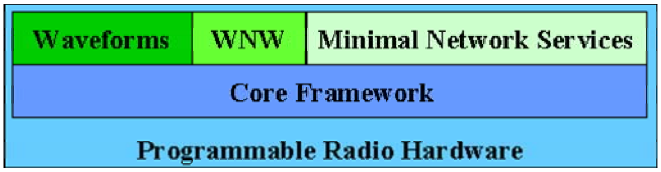


Figure 33. SCA integration of JTR Set Components[92]

### 3. Control and Provisioning of Wireless Access Point (CAPWAP) Tunneling Protocol - CTP

Lastly, the Control and Provisioning of Wireless Access Point (CAPWAP) Tunneling Protocol (CTP) concept should also prove beneficial to UWAP development. CTP is a follow-on technology designed to replace the Light Weight Access Point Protocol (LWAPP). LWAPP can be thought of as taking the brains out of an AP and placing them in a central management system (e.g., WLAN switch, router, etc). In essence, what you are doing is turning a fat (traditional/commonly used) AP into a thin AP (in other words, a remote RF extension to a controlling switch or router).[93]

On the other hand, CTP, though similar to LWAPP, claims to provide interoperability between WAPs straight out of the box. This protocol is considered open

[91] JTRS, *JTRS Technical Overview*, http://jtrs.army.mil/sections/technicalinformation/fset_technical_sca.html, Last accessed 13 Feb 06.

[92] From: Ibid.

[93] TechWorld, *What's behind the CAPWAP flap?*, http://www.techworld.com/mobility/features/index.cfm?FeatureID=480, Last accessed 10 Mar 06.

architecture and is said to be highly adaptable to diversified networks and offers seamless roaming (over L3) between different technology based APs and between APs and their associate access routers (also known as an access controller). This protocol, in addition to providing greater mobility across subnets and supporting low-latency roaming, allows thin APs to act intelligently. However, the greatest difference between LWAPP and CTP is LWAPP only supports 802.11 standards while CTP supports 802.11 and other wireless technologies (e.g., 802.15, 802.16) that are CTP compliant.[94]

The IETF (Internet Engineering Task Force) produced an Operations Group Internet Draft pertaining to CTP, stating that this tunneling protocol "allows for the centralized control and provisioning of a large number of wireless access points from access controllers." It continued to declare that CTP:

> …is supported by an architecture where the MAC layer of the RF technology is terminated within the AP. This allows the protocol to be extensible to multiple radio technologies. It assumes an IP connection between the access points and access controllers and has signaling primitives to enable wireless station mobility between access points. Therefore, seamless Layer 3 subnet mobility is seamlessly enabled by this protocol.[95]

In our opinion, further research in one or more of these areas will undoubtedly aid in the development of the optimum Universal Wireless Access Point (UWAP/UAP) solution. Ultimately, this solution, the Universal Wireless Access Point, will bring tremendous battlefield advantage to U.S. and Coalition forces operating in a joint, multi-national, hasty forming, heterogeneous and mobile networking environment.

## C. APPLICATION OF HOW "JOINT POINT" TECHNOLOGY MAY BE EMPLOYED IN A TACTICAL NETWORK ENVIRONMENT

As mentioned in Chapter I and as depicted in Figure 34 below, there are multitudes of mobile, wireless nodes simultaneously operating within TNT's mesh enabled environmental test bed. However, as a result of product limitations, only the

[94] Chantry Networks, *Chantry Networks and Propagate Networks Partner to Propose an Alternative Standard to Expired LWAPP Protocol,* http://www.chantry.webeditz.com/news/detail.php?ID=36, Last accessed 10 Mar 06.

[95] Internet Engineering Task Force (IETF) Operations Group Internet Draft, *CAPWAP Tunneling Protocol (CTP),* http://tools.ietf.org/wg/capwap/draft-singh-capwap-ctp/draft-singh-capwap-ctp-02.txt, Last accessed 12 Mar 06.

remote nodes and the APs that are loaded with the same technology (e.g., 802.11, ITT MEA) have the able to pass data between themselves. In other words, an AP built on 802.11 technology will not be able to understand the data frames received from a remote node that is trying to communicate using ITT MEA technology.

In efforts to mitigate this display of interoperability from the CR NOC's perspective, multiple APs of diverse technologies (e.g., 802.11, ITT MEA, etc) were connected to the infrastructured network. This created entry points for data to be transmitted to or received from any of the wireless nodes operating within the TNT wireless network boundary. From an operational stand point, having multiple APs interfacing with your infrastructured network is perfectly feasible; however, this arrangement does not demonstrate an efficient use of network management or configuration. Similarly, the LRV (mobile TOC) was equipped with multiple AP devices. Unlike the CR NOC, the mobile TOC does not have the room to accommodate a configuration consisting of a large number of APs. This limitation substantially reduces the mobile TOCs effectiveness by restricting its payload to one specific AP (i.e., 802.11, 802.16, 802. 20 or ITT MEA) or if a switch is added, to the number of APs accommodated by the switch and by the physical space available in the LRV. Another remote node, the tactical balloon, which can serve as both a reconnaissance platform and a wireless relay station, is equally affected by the inability to communicate with devices loaded with dissimilar wireless technologies. Analogous to the LRV, the balloon can be used to provide data, video feeds and/or to extend the mesh beyond normal line-of-sight propagation constraints. Failure in performing such routine tasks weighs heavenly against the NOCs forward looking reconnaissance and extended communications support capabilities.

These and other limitations can easily be overcome by implementing a device that has the functionality of a Universal Wireless Access Point (UWAP/UAP) as outlined in this thesis. Referring back to the problem scenarios mentioned above, numerous mission enhancement capabilities are projected after UWAP/UAP implementation. The initial benefits in replacing the various APs located at CR NOC with a UAP can be seen from a network configuration and management view point. UAP implementation at this level will:

(1) eliminate the guess work between mission planners and system engineers when they coordinate the requirements to design and build a network configuration scheme.

(2) the storage, inventory, and material management responsibilities will become less complicated during setup and teardown evolutions.

(3) network troubleshooting time and complexity level will also decrease as a result of fewer components interacting with the network, and

(4) personnel and parts support requirements to maintain several different types of AP devices will be reduced.

Benefits also exist at the tactical level. Using a UAP, NOC/TOC Commanders no longer are burden to identify every possible flavor of wireless technologies they expect to operate with prior to system deployment because the UAP will have the capability to be reconfigured remotely to accept new technologies. Pertaining to the LRV, installing a UAP at this echelon will mainly enhance its mission capabilities by allow mission planners to utilize this platform to provide reach back continuity for wireless node deployed within TNT. This capability can also be stated as allowing "n" number of heterogeneous mesh networks the ability to connect to the NOC and/or another mesh network as indicated in Figure 34 below. The blue shaded areas in Figure 34 indicates projected UAP implementation sites. Having a device which can link to a variety of wireless technologies, known or unknown, now allows this vehicle to be multitasked. Lastly, outfitting the tactical balloons with such a device will likewise provide another reliable reach back link for remote nodes regardless of their wireless technology.

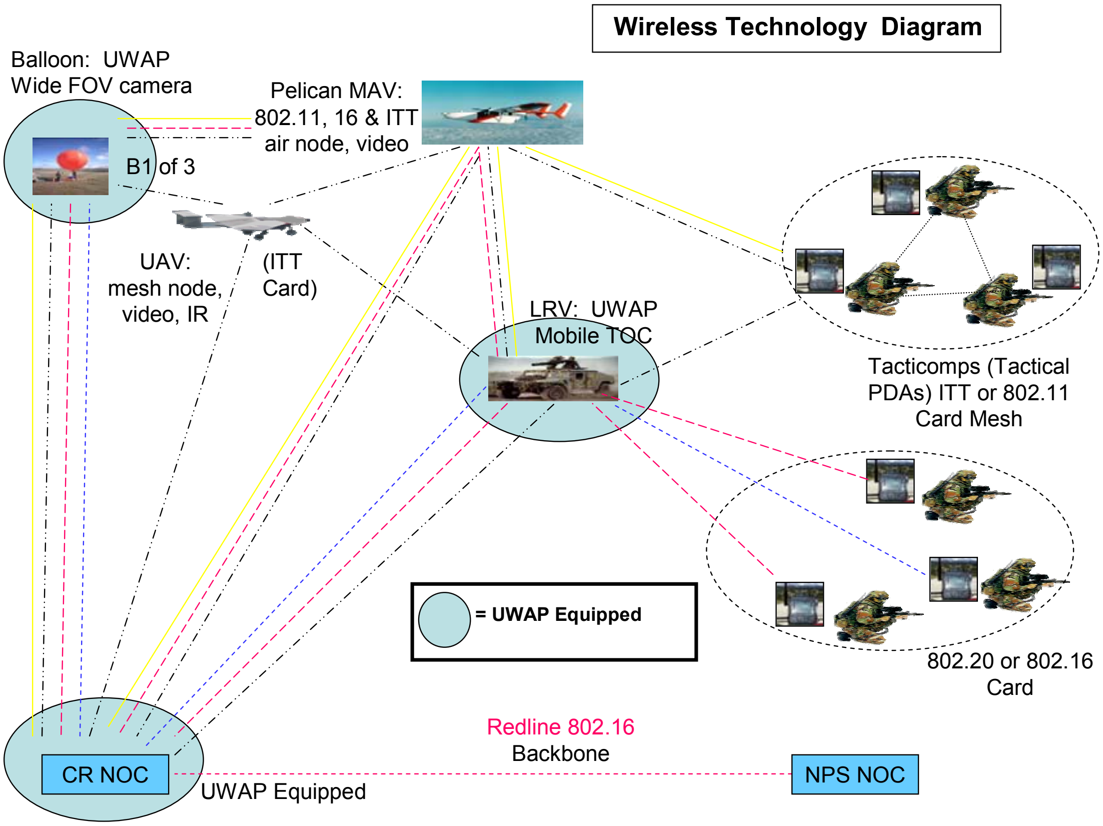


Figure 34. TNT Wireless Mesh Network Layout Equipped with UWAPs

From a global/multinational standpoint, where adaptation and interoperability is paramount and time critical, the UAP will be a key component in providing ubiquitous and continuous communication connectivity to the war-fighter. Regardless of the wireless technology utilized, every valid, wireless member within range of the UWAP will be able to access the network and communicate with both wired and wireless members of the network to include wireless members with dissimilar wireless technologies. System integration and/or compatibility limitations will be alleviated thus reducing communication delays/denials and increase asset (manpower/equipment) availability across the board. Mobile gateway platforms can be quickly and easily integrated into any wireless configuration with minimum system administration support. Being able to deploy faster and lighter will produce great dividends to tactical users in any mobile or semi-static, tactical environment. In conclusion, the application of universal wireless joint point technology (e.g., UWAP, UAP) in supports of joint, coalition or multinational tactical operations will provide the war-fighter the capability to transmit, receive, and bridge digital signal among diverse and dissimilar waveforms and network protocols within the wireless local area network (WLAN), wide area network (WWAN ), cellular, and possibly satellite frequency spectrum.

# LIST OF REFERENCES

1. Planet3 Wireless, CWNA Certified Wireless Network Administrator Official Study Guide (Exam PWO-100) 3rd Edition, McGraw-Hill and Osborne, 2005.

2. VICOMSOFT Corporation, Support–White Papers–Wireless Networking, http://www.vicomsoft.com/knowledge/reference/wireless1.html#1, Last accessed 05 Oct 05.

3. Corson, S. and others, *Mobile Ad hoc Networking (MANET),* RFC 2501, Internet Engineering Task Force (IETF), Jan 99.

4. Wikipedia, The Free Encyclopedia, http://en.wikipedia.org/wiki/Wireless_access_point, Last accessed 06 Oct 05.

5. Wikipedia, The Free Encyclopedia, http://en.wikipedia.org/wiki/Hotspot_%28wifi%29, Last accessed 10 Dec 05.

6. Dr. Creese, Sadie and others, *Interopability Challenges for Wireless Communication*, QinetiQ, 31 Mar 03, http://www.nextwave.org.uk/downloads/forward_icwc.pdf, Last accessed 10 Dec 05.

7. Wikipedia, The Free Encyclopedia, http://www.webopedia.com/TERM/D/DSSS.html, Last accessed 08 Nov 05.

8. Wikipedia, The Free Encyclopedia, http://www.webopedia.com/TERM/O/OFDM. html, Last accessed 08 Nov 05.

9. Linksys Wireless-G WAP54G 802.11b/g Wireless Access Point: Product Features, http://www.dealtime.com/xPF-Linksys_Wireless_G_Access_Point_WAP54G, Lasted accessed 10 Dec 05.

10. Mesh Networks, *Mobile Broadband Network Solutions*, Meshnetworks, Inc., 2002, http://www.now.co.uk/v2/wireless/meshnetworks/files/datasheet.pdf, Last accessed 10 Dec 05.

11. Redline Communications, *Datasheet: AN-50e Wireless Broadband,* Redline Communications Inc., Last accessed 10 Dec 05.

12. Smith, Eric, *MeshNetworks Gets FCC Approval*, 13 Nov 02, http://www.wi-fiplanet.com/news/ article.php/1500101, Last accessed 23 Jan 06.

13. Mesh Networks, IAP6300 Intelligent Access Point Brochure, MeshNetworks, Inc, 2002, http://www.cwti.us/brochure/CWTI-Technology_Mesh-IAP6300.pdf, Last access 10 Dec 05.

14. Parish, William J. and Tovar, Daniel R., *Tactical Wireless Networking in Coalition Environments: Implementing an IEEE 802.20 Wireless End-User Network Utilizing Flash-OFDM to Provide a Secure Mobile Extension to Existing WAN*, Master's Thesis, Naval Postgraduate School, Monterey, California, Sep 05.

15. Flarion, Product and Technology: RadioRouter Base Station, Flarion Technologies Inc., 2003-2005, http://www.flarion.com/products/radio_router.asp, Last accessed 10 Dec 05.

16. Flarion, Product and Technology: Wireless Network Cards, Flarion Technologies Inc., 2003-2005, http://www.flarion.com/products/cards.asp, Last accessed 10 Dec 05.

17. Siva C., Murthy R. and Manoj, B. S., Ad Hoc Wireless Networks: Architecture and Protocols, Prentice Hall PTR, 2004.

18. Iowa State University – Department of Computer Science, http://www.cs.iastate.edu/~cs586/f04/notes/ chapter4_2.pdf, Last accessed 20 Dec 05.

19. Mosawi, T. Al and others, *Centre for Telecommunications Research - Review of Existing Mobile Broadband Wireless Access (MBWA) Technologies (IEEE 802.16 and IEEE 802.20),* King's College London - University of London, Nov 04.

20. Flarion Technologies, Inc., *Whitepaper – OFDM for Mobile Data Communications,* http://www.flarion.com/products/whitepapers/OFDM_Mobile_Data_Communications.pdf. Mar 2003, Last accessed 23 Dec 05.

21. IEEE Standards Association, http://grouper.ieee.org/groups/802/20/WG_Docs/ 802.20-03-16r1.ppt, Last accessed 27 Dec 05.

22. IEEE 802, LAN/MAN Standards Committee, http://www.ieee802.org/1/linksec/Docs/ LAN_Threat_Assessment_Rev.1.doc, Last accessed 22 Dec 05.

23. Varshney, Upkar and Jain, Radhika, *Issues in Emerging 4G Wreless Networks*, Georgia State University, http://www.ee.oulu.fi/~skidi/teaching/mobile_and_ ubiquitous_multimedia_2002/ issues_in_emerging_4G_wireless_networks.pdf, Last accessed 05 Dec 05.

24. Abuelma'atti, Omar, Merabti, Madjid and Askwith, Bob, *Interworking the Wireless Domain*, Liverpool John Moores University, http://www.scit.wlv.ac.uk/~jphb/cp4040/rolandonotes/CSNDSP2002/ Papers/J1/J1.1.pdf, Last accessed 15 Jan 06.

25. Wikipedia, The Free Encyclopedia, http://en.wikipedia.org/wiki/General_Packet_Radio_ Service, Last accessed 17 Feb 06.

26. Webopedia, http://www.webopedia.com/TERM/U/UMTS.html, Last accessed 17 Feb 06.

27. Aguero, Ramon and others, *Multi-Radio Access in Ambient Networks*, Wireless World Initiative Whitepaper and Presentation, 08 Nov 05.

28. Tao, Zhongping, Bochmann, Gregor V., and Dssouli, Rachida, *A Formal Method for Synthesizing Optimized Protocol Converters and its Application to Mobile Data Networks,* Mobile Networks and Application 2, Baltzer Science Publishers, 1997.

29. Varshney, Upkar, *Network Access and Security Issues in Ubiquitous Computing*, George State University, http://weatherhead.cwru.edu/pervasive/Paper/UBE%202003%20-%20Varshney.pdf, Last accessed 03 Jan 06.

30. Green, Paul E. Jr., *Protocol Conversion*, IEEE Transactions on Communications, Vol. Com-34, No. 3, Mar 86.

31. Software Defined Radio Forum, *SDR Brochure*, http://www.sdrforum.org/sdr_brochure_10_24_02.pdf, Last accessed 17 Jan 06.

32. McCarthy, Darren, *Software-defined Radio: Integration for Innovation*, RFDesign, Sep 05, 44, http://rfdesign.com/mag/0509RFDF4.pdf, Last accessed 17 Jan 06.

33. Hickling, Ronald M., *New Technology Facilities True Software-defined Radio*, RFDesign, Apr 05, 18, http://rfdesign.com/mag/504rfdf1.pdf, Last accessed 17 Jan 06.

34. Chevillat, P. R. and Schott, W., *Broadband Radio LANs and the Evolution of Wireless Beyond 3G, IBM Journal of Research and Development, Volume 47, Number 2/3*, March/May 2003, International Business Machines Corporation.

35. InMotion Technology, *Mobile LAN: Enabling Applications on the Edge*, An InMotion Whitepaper 2005.

36. Webopedia, http://www.webopedia.com/TERM/H/HSDPA.html, Last accessed 21 Feb 06.

37. Wikipedia, The Free Encyclopedia, http://en.wikipedia.org/wiki/WiDEN, Last accessed 21 Feb 06.

38. OnBoard Mobile Gateway, *Mobile WLAN: The Next Generation Wireless Platform for Public Safety,* http://www.inmotiontechnology.com/oMG%201000%20Data%20 Sheet.pdf, Last accessed 10 Feb 06.

39. NETGEAR, Inc., *Reference Manual for the Mobile Broadband Router (MBR) 814*, Netgear, Inc. 2005.

40. Vanu Software Radio, *Addressing the Complexities of Software Defined Radio (SDR)*, http://h71028.www7.hp.com/enterprise/downloads/SDR_SolutionBrief.pdf, Last accessed 09 Feb 06.

41. VANU, *The Anywave Base Station*, http://vanu.com/products/basestation.html, Last accessed 12 Feb 06.

42. VANU, *Vanu, Inc Announces the First Commercial Software Radio Deployment in Canada*, http://vanu.com/news/prs/ICEWirelessFinal.pdf, Last accessed 12 Feb 06.

43. PRISMTECH, *Software Defined Radio SDR*, http://www.prismtechnologies.com/section-item.asp?sid4=&sid3=&sid2=6&sid=17&id=73, Last accessed 12 Feb 06.

44. Miercom, *Lab Testing Summary Report*, http://www.cisco.com/application/pdf/en/us/ guest/products/ps5854/c1244/cdccont_0900aecd8017382b.pdf, Report 040903, September 2004, Last accessed 21 Feb 06.

45. Cisco Systems, *Model Comparison*, http://www.cisco.com/en/US/products/ps5854/prod_models_comparison.html, Last accessed 21 Feb 06.

46. Cisco Systems, *Cisco System Integrated Service Routers*, http://www.cisco.com/cdc_content_elements/flash/nextgen/webversion/portfolio/demo.htm?NO_NAV, Last accessed 21 Feb 06.

47. Cisco Systems, *Cisco 2811Integrated Services Router*, http://www.cisco.com/en/US/products/ps5881/index.html, Last accessed 21 Feb 06.

48. Cisco System, *Wireless Services on the Cisco 800, 1800, 2800, and 3800 Series Integrated Services Router Date Sheet,* http://www.cisco.com/application/pdf/en/us/guest/products/ps5854/c1650/cdccont_0900aecd8016ef57.pdf, Last accessed 25 Jan 06.

49. CellularOnline, *Flash-OFDM (Orthogonal Frequency Division Multiplexing)*, http://www.cellular.co.za/flash-ofdm.htm, Last accessed 27 Jan 06.

50. Flarion, *FLASH-OFDM Technology*, http://www.flarion.com/products/flash_ofdm.asp, Last accessed 25 Jan 06.

51. Flarion, *The FLASH-OFDM System*, http://www.flarion.com/about/default.asp, Last accessed 04 Feb 06.

52. Cisco Systems, Inc., *Cisco HWIC-AP WLAN Module for Cisco 1800 (Modular)*, Cisco 2800 and Cisco 3800 Series Integrated Services Routers Data Sheet, 1995-2000.

53. NETGEAR, Inc., *MBR14XF 802.11g FLASH-OFDM Mobile Broadband Router*, http://www.netgear.com/pdf_docs/MBR814XF_ds_r2_2Sep05.qxd.pdf, Last accessed 14 Mar 06.

54. Ramon Aguero, *Multi-Radio Access in Ambient Networks*, Wireless World Initiative 2005.

55. Joachim Sachs and others, *A Generic Link Layer for Future Generation Wireless Networking*, http://ieeexplore.ieee.org/iel5/8564/27114/01204448.pdf?arnumber=1204448, 835-36, Last accessed 03 Jan 06.

56. Stefan Aust and others, *Policy Based Mobile IP Handoff Decision (POLIMAND) Using Generic Link Layer Information*, http://www.iponair.de/publications/Aust_MWCN2003.pdf, 3, Lasted accessed 07 Feb 06.

57. Boeing, *Integrated Defense System*, http://www.boeing.com/defense-space/ic/jtrs/index.html, Last accessed 16 Feb 06.

58. JTRS, *JTRS Technical Overview*, http://jtrs.army.mil/sections/technicalinformation/fset_technical_sca.html, Last accessed 13 Feb 06.

59. TechWorld, *What's behind the CAPWAP flap?*, http://www.techworld.com/mobility/features/index.cfm?FeatureID=480, Last accessed 10 Mar 06.

60. Chantry Networks, *Chantry Networks and Propagate Networks Partner to Propose an Alternative Standard to Expired LWAPP Protocol,* http://www.chantry.webeditz.com/news/detail.php?ID=36, Last accessed 10 Mar 06.

61. Internet Engineering Task Force (IETF) Operations Group Internet Draft, *CAPWAP Tunneling Protocol (CTP),* http://tools.ietf.org/wg/capwap/draft-singh-capwap-ctp/draft-singh-capwap-ctp-02.txt, Last accessed 12 Mar 06.

THIS PAGE INTENTIONALLY LEFT BLANK

# INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Dan Boger
   Naval Postgraduate School
   Monterey, California

4. Dave Netzer
   Naval Postgraduate School
   Monterey, California

5. Alexander Bordetsky
   Naval Postgraduate School
   Monterey, California

6. LCDR Gordon Cross
   USSOCOM/SOKF-J9
   7701 Tampa Point Blvd
   MacDill AFB, FL 33621-5323

7. Erik Syvrud
   2907 Bay to Bay Blvd., Suite 100
   Tampa, FL 33621